Key rate of quantum key distribution with hashed two-way classical communication*

Shun Watanabe,† Ryutaroh Matsumoto,‡ and Tomohiko Uyematsu§
Department of Communicaiton and Integrated Systems
Tokyo Institute of Technology
2-12-1, Oookayama, Meguro-ku,
Tokyo, 152-8552, Japan

Yasuhito Kawano¶
NTT Communication Science Laboratories,
NTT Corporation
3-1, Wakamiya, Morinosato, Atsugishi,
Kanagawa Pref., 243-0198, Japan

We propose an information reconciliation protocol that uses two-way classical communication. The key rates of quantum key distribution (QKD) protocols that use our new protocol are higher than those of previously known protocols for a wide range of error rates for the BB84 and six-state protocols. We also clarify the relation between the proposed and known QKD protocols, and the relation between it and entanglement distillation protocols (EDPs).

PACS numbers: 03.67.Dd, 89.70.+c

I. INTRODUCTION

Quantum key distribution (QKD) protocols provide a way for two parties, a sender, Alice, and a receiver, Bob, to share an unconditionally secure key in the presence of an eavesdropper, Eve. Unlike conventional schemes of key distribution that rely on unproven computational assumptions, the security of QKD protocols is guaranteed by the principles of quantum mechanics.

QKD protocols usually consist of two parts, a quantum and a classical part. Alice sends a binary sequence to Bob in the quantum part by encoding it into quantum states that are randomly chosen from a set of non-orthogonal states. Since unknown non-orthogonal states cannot be cloned perfectly, any eavesdropping attempt by Eve will disturb the transmitted quantum states. Thus, by estimating the error rate of the transmitted quantum states, Alice and Bob can estimate the amount of information that Eve has gained. For the sequence that remains after the error estimation phase, which is usually called the raw key, Alice and Bob first carry out an information reconciliation (IR) protocol [1] to share the same bit sequence. Alice and Bob then distill the final secure key by conducting a privacy amplification (PA) protocol [2].

The best-known QKD protocols are the Bennett-Brassard 1984 (BB84) protocol [3] and the six-state protocol [4]. The unconditional security of the BB84 protocol has been proved [5, 6, 7]. Shor and Preskill [8] presented a simple proof of the BB84 protocol by showing that the QKD protocol that uses the entanglement distillation protocol (EDP) [9, 10] can be converted into the BB84 protocol. After that, the unconditional security of the six-state protocol was proved [11] by using the same technique as Shor and Preskill used [8]. Recently, the security of generic QKD protocols that include the BB84 protocol and the six-state protocol has been proved [12, 13, 14], which are based on information theoretical techniques instead of Shor and Preskill's technique.

In addition to the security of QKD protocols, the key rates of QKD protocols are also important, where the key rate is defined by the ratio of the length of the final secure key to the length of the raw key. Gottesman and Lo [15] converted EDPs that use two-way classical communication into QKD protocols that use the same communication. More specifically, they proposed preprocessing that uses two-way classical communication. By inserting this two-way preprocessing before the conventional one-way IR protocol, the key rates of QKD protocols are increased when the error rate of a channel expressed as a percentage is more than about 9 %. Indeed, the tolerable error rate of the BB84 protocol is increased from 11 % to 18.9 %, and that of the six-state protocol is increased from 12.7 % to 26.4 %, where the tolerable error rate is the error rate at which the key rate becomes zero. Chau later showed that the two-way BB84 protocol can tolerate 20.0 % error rate, and that the two-way six-state protocol can tolerate 27.6 % error rate [16]. Recently, this kind of two-way preprocessing has been applied to QKD protocols with weak coherent pulses [17, 18]. It should be noted that this preprocessing is also known within the classical key agreement context, in which it is usually called an advantage distillation protocol [19]. Bae and Acín and Acín et al. [20, 21] extensively studied

*Part of this paper will be presented at the 2007 IEEE International Symposium on Information Theory, Acropolis Congress and Exhibition Center, Nice, France, 24th–29th June 2007, and will be published in its proceedings without proofs.
†Electronic address: shun-wata@it.ss.titech.ac.jp
‡Electronic address: ryutaroh@rmatsumoto.org; URL: http://www.rmatsumoto.org/research.html
§Electronic address: uyematsu@ieee.org
¶Electronic address: kawano@theory.brl.ntt.co.jp

the noise tolerance of QKD protocols with advantage distillation protocols, on the other hand, we are interested in the key rates of QKD protocols in this paper.

Vollbrecht and Vestraete proposed a new type of two-way EDP [22]. This protocol uses previously shared EPR pairs as an assistant resource (two-way breeding EDP), and the distillation rate of this EDP exceeds that of one-way EDPs for a whole range of fidelities, where a fidelity is that between the initial mixed state and the EPR pair. Using the fact that a breeding EDP can be converted into a QKD protocol assisted by one-time pad encryption with a pre-shared secret key [23], Vollbrecht and Vestraete's two-way breeding EDP [22] was converted into a two-way QKD protocol assisted by one-time pad encryption [17, 24]. The key rate of the converted QKD protocol is higher than that of one-way QKD protocols [8, 11] for a whole range of error rates. It should be noted that the use of a pre-shared secret key is not the basis of their improvement, because any QKD protocol that makes use of a pre-shared key can be transformed into an equally efficient protocol that does not need a pre-shared secret key [25].

We propose an IR protocol that uses two-way classical communication in this paper. Our proposed protocol is based on Vollbrecht and Vestraete's idea of two-way breeding EDP [22], but does not require any pre-shared secret keys. Furthermore, our protocol does not leak information that is redundantly leaked to Eve [17, 24]. More precisely, in these protocols [17, 24], Alice sends a redundant message that is useless to Bob, but is useful to Eve. However, in the proposed protocol, Alice does not send that redundant information. As a result, for the BB84 and six-state protocol, the key rates of the QKD protocols that use our IR protocol are higher than those of previously known protocols for a wide range of error rates. Especially, the key rate of our protocol is higher than those of known protocols [8, 11, 13, 24] for the whole range of error rates. We also show the relation between the proposed protocol and the advantage distillation protocol, i.e., the B-step of Gottesman and Lo [15] (Remark 4). We also show the relation between the proposed QKD protocol and Vollbrecht and Vestraete's EDP. As a results, it turns out that there does not seem to be any EDP that corresponds to our proposed protocol (Remark 5).

The rest of this paper is organized as follows. Section II proposes a two-way IR protocol. Section III presents the key rate formula of the QKD protocol that uses our proposed IR protocol. There is a proof of the key rate formula in the Appendix D. Section IV presents the key rate formula as a function of error rate. The proof of this formula is presented in Appendix E.

II. TWO-WAY INFORMATION RECONCILIATION PROTOCOL

We propose an IR protocol that uses two-way classical communication (called two-way IR protocol after this) in this section. When Alice and Bob have correlated classical sequences, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{2n}$, the purpose of IR protocols for Alice and Bob is to share the same classical sequence by exchanging messages over a public authenticated channel, where $\mathbb{F}_2$ is the field of order 2. Here, we assume that the pair of sequences $(\mathbf{x}, \mathbf{y})$ is independently identically distributed (i.i.d) according to a joint probability distribution, P_{XY}, on $\mathbb{F}_2 \times \mathbb{F}_2$.

Let us review some notations for a linear code to describe our IR protocol. An $[n, n-m]$ linear code, $\mathcal{C}_{n,m}$, is an $(n-m)$-dimensional linear subspace of $\mathbb{F}_2^n$. Then, a parity check matrix, $M_{\mathcal{C}_{n,m}}$, of code $\mathcal{C}_{n,m}$ is an $m \times n$ matrix of rank m with $0, 1$ entries such that $\mathbf{c} M_{\mathcal{C}_{n,m}}^T = \mathbf{0}$ for any $\mathbf{c} \in \mathcal{C}_{n,m}$, where $M_{\mathcal{C}_{n,m}}^T$ is the transpose matrix of $M_{\mathcal{C}_{n,m}}$. A decoder, $g_{\mathcal{C}_{n,m}}$, of code $\mathcal{C}_{n,m}$ is a map from a syndrome, $\mathbf{t} \in \mathbb{F}_2^m$, to an error, $\mathbf{e} \in \mathcal{D}(\mathbf{t})$, where $\mathcal{D}(\mathbf{t}) := \{\mathbf{e} \in \mathbb{F}_2^n \mid \mathbf{e} M_{\mathcal{C}_{n,m}}^T = \mathbf{t}\}$ is the set of errors whose syndromes are $\mathbf{t}$. After this, we will assume that a linear code is implicitly specified with a parity check matrix and a decoder.

We need to define some auxiliary random variables to describe our IR protocol. Let $\xi_1 : \mathbb{F}_2^2 \to \mathbb{F}_2$ be a function defined as $\xi_1(a_1, a_2) := a_1 + a_2$ for $a_1, a_2 \in \mathbb{F}_2$, and let $\xi_2 : \mathbb{F}_2^2 \to \mathbb{F}_2$ be a function defined as $\xi_2(a, 0) := a$ and $\xi_2(a, 1) := 0$ for $a \in \mathbb{F}_2$. For a pair of joint random variables $((X_1, Y_1), (X_2, Y_2))$ with a distribution, P_{XY}^2, define random variables $U_1 := \xi_1(X_1, X_2)$, $V_1 := \xi_1(Y_1, Y_2)$ and $W_1 := U_1 + V_1$. Furthermore, define random variables $U_2 := \xi_2(X_2, W_1)$, $V_2 := \xi_2(Y_2, W_1)$ and $W_2 := U_2 + V_2$. For the pair of sequences, $\mathbf{x} = (x_{11}, x_{12}, \ldots, x_{n1}, x_{n2})$ and $\mathbf{y} = (y_{11}, y_{12}, \ldots, y_{n1}, y_{n2})$, which is distributed according to the product distribution, P_{XY}^{2n}, let $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$ be $2n$-bit sequences such that

$$u_{i1} := \xi_1(x_{i1}, x_{i2}), \quad v_{i1} := \xi_1(y_{i1}, y_{i2}), \quad w_{i1} := u_{i1} + v_{i1}$$

and

$$u_{i2} := \xi_2(x_{i2}, w_{i1}), \quad v_{i2} := \xi_2(y_{i2}, w_{i1}), \quad w_{i2} := u_{i2} + v_{i2}$$

for $1 \leq i \leq n$. Then, the pair $(\mathbf{u}, \mathbf{v})$ is distributed according to the distribution, $P_{U_1U_2V_1V_2}^n$, and the discrepancy, $\mathbf{w}$, between $\mathbf{u}$ and $\mathbf{v}$ is distributed according to the distribution, $P_{W_1W_2}^n$. For sequence $\mathbf{w}$, let $\mathsf{T}_b := \{j \mid 1 \leq j \leq n,\ w_{j1} = b\}$ be the set of indices of blocks such that the parities of the discrepancies are b. For the subsequence, $\mathbf{u}_2 := (u_{12}, \ldots, u_{n2})$, let $\mathbf{u}_{2,\mathsf{T}_b}$ be the subsequence that consists of the i-th bit of $\mathbf{u}_2$ such that $i \in \mathsf{T}_b$.

Well-known methods [15, 19, 22] of two-way processing within the key distillation context have been to classify blocks of length 2 according to the parity, w_{i1}, of the discrepancies in each block. In conventional two-way processing of the key distillation protocols [15, 19],

which is so-called advantage distillation protocols, Alice sends the parity sequence, $\mathbf{u}_1 := (u_{11}, \ldots, u_{n1})$, to Bob so that he can identify the parity sequence, $\mathbf{w}_1 := (w_{11}, \ldots, w_{n1})$, of the discrepancies. Then, Alice and Bob discard $\mathbf{u}_1$ and $\mathbf{v}_1 := (v_{11}, \ldots, v_{n1})$ respectively, because $\mathbf{u}_1$ is revealed to Eve. Furthermore, Alice and Bob discard the second bit of the i-th block, if the parity of the discrepancies is 1, i.e., $i \in \mathsf{T}_1$. Finally, Alice and Bob undertake an error correction procedure for the subsequences $(\mathbf{u}_{2,\mathsf{T}_0}, \mathbf{v}_{2,\mathsf{T}_0})$. More precisely, Alice sends the syndrome, $\mathbf{t}_2 := \mathbf{u}_{2,\mathsf{T}_0} M^T_{\mathcal{C}_{n_0,m_0}}$, for the prescribed $[n_0, m_0]$-linear code, and then Bob decodes $\hat{\mathbf{w}}_{2,\mathsf{T}_0} := g_{\mathcal{C}_{n_0,m_0}}(\mathbf{t}_2 + \mathbf{v}_{2,\mathsf{T}_0} M^T_{\mathcal{C}_{n_0,m_0}})$ and obtains $\mathbf{v}_{2,\mathsf{T}_0} + \hat{\mathbf{w}}_{2,\mathsf{T}_0}$, where $n_0 := |\mathsf{T}_0|$ is the cardinality of the set, T_0.

Our two-way IR protocol, which is based on Vollbrecht and Vestraete's idea of two-way EDP [22], is quite similar to the previously described two-way processing except for one significant change. As is usual in information theory, if we allow negligible error probability, Alice does not need to send the parity sequence, $\mathbf{u}_1$, to Bob to identify parity sequence $\mathbf{w}_1$. More precisely, Bob can decode $\mathbf{w}_1$ with negligible decoding error probability if Alice sends a syndrome, $\mathbf{t}_1 := \mathbf{u}_1 M^T_{\mathcal{C}_{n,m}}$, for a linear code such that the rate is $\frac{m}{n} \simeq H(P_{W_1})$ [26, Corollary 2]. Since Eve's available information from syndrome $\mathbf{t}_1$ is much smaller than that from sequence $\mathbf{u}_1$ itself, our IR protocol is more efficient than the above-mentioned two-way processing in most cases, which will be discussed in Section IV. Our IR protocol is formally executed as follows, where the tilde ˜ and hat ˆ on a sequence, a set or a number indicate that they are guessed versions of those without these superscripts. Note that the inputs of the IR protocol are Alice's bit sequence $\mathbf{x}$ and Bob's bit sequence $\mathbf{y}$, and the outputs of the IR protocol are a sequence, $\hat{\mathbf{u}}$, guessed by Alice and a sequence, $\tilde{\mathbf{u}}$, guessed by Bob.

(i) Alice locally computes $\mathbf{u}_1$ and Bob does the same for $\mathbf{v}_1$.

(ii) For a prescribed $[n, n-m]$ linear code, $\mathcal{C}_{n,m}$, Alice sends syndrome $\mathbf{t}_1 = \mathbf{u}_1 M^T_{\mathcal{C}_{n,m}}$ to Bob.

(iii) Bob decodes $\hat{\mathbf{w}}_1 := g_{\mathcal{C}_{n,m}}(\mathbf{t}_1 + \mathbf{v}_1 M^T_{\mathcal{C}_{n,m}})$, and sends $\hat{\mathbf{w}}_1$ to Alice.

(iv) Alice computes $\hat{\mathbf{u}}_2$. If the number, $\hat{n}_0 := |\{i \mid \hat{w}_{i1} = 0\}|$, of blocks such that the guessed parity, $\hat{w}_{i1}$, of the discrepancies is 0 does not satisfy $\underline{n}_0 \le \hat{n}_0 \le \overline{n}_0$ for prescribed integers, $\underline{n}_0$ and $\overline{n}_0$, then Bob randomly guesses $\hat{\mathbf{u}}_{2,\hat{\mathsf{T}}_0}$. Otherwise, Alice sends the syndrome, $\hat{\mathbf{t}}_2 := \hat{\mathbf{u}}_{2,\hat{\mathsf{T}}_0} M_{\mathcal{C}_{\hat{n}_0,\hat{m}_0}}$, for a prescribed $[\hat{n}_0, \hat{n}_0 - \hat{m}_0]$ linear code, $\mathcal{C}_{\hat{n}_0,\hat{m}_0}$.

(v) Bob decodes $\tilde{\mathbf{w}}_{2,\hat{\mathsf{T}}_0} := g_{\mathcal{C}_{\hat{n}_0,\hat{m}_0}}(\hat{\mathbf{t}}_2 + \hat{\mathbf{v}}_{2,\hat{\mathsf{T}}_0} M^T_{\mathcal{C}_{\hat{n}_0,\hat{m}_0}})$, and obtains $\tilde{\mathbf{u}}_{2,\hat{\mathsf{T}}_0} := \hat{\mathbf{v}}_{2,\hat{\mathsf{T}}_0} + \tilde{\mathbf{w}}_{2,\hat{\mathsf{T}}_0}$.

Note that $\hat{\mathbf{u}}_{2,\hat{\mathsf{T}}_1}$ and $\hat{\mathbf{v}}_{2,\hat{\mathsf{T}}_1}$ are set to all 0s in our protocol, which is mathematically equivalent to discarding them.

According to the universal channel coding theorem for the linear code [26, Corollary 2], rates $\frac{m}{n} = H(P_{W_1}) + \delta$ and $\frac{\hat{m}_0}{\hat{n}_0} = H(P_{W_2|W_1=0}) + \delta$ for small $\delta > 0$ are sufficient for Bob to decode $\mathbf{w}_1$ and $\mathbf{w}_{2,\mathsf{T}_0}$ with negligible decoding error probability. Furthermore, we set $\underline{n}_0 := n(P_{W_1}(0) - \delta)$ and $\overline{n}_0 := n(P_{W_1}(1) + \delta)$ to satisfy the condition, $\underline{n}_0 \le \hat{n}_0 \le \overline{n}_0$, in Step (iv) with high probability.

Remark 1 Since we cannot estimate the probability distribution of error exactly in QKD protocols and the actual distribution fluctuates around the estimated error distribution, universality of codes is required. Even though the distribution of errors in the QKD protocols are not necessarily i.i.d., it is sufficient to consider a universality condition on codes for the i.i.d. case. More precisely, it is sufficient to use a linear code such that the decoding error probability of the linear code is universally small for any binary symmetric channel whose crossover probability is close to the estimated error rate. Such observations were first pointed out by Hamada [27]. Efficiently decodeable linear codes such as the low density parity check matrix code [28] and the turbo code [29] satisfy this condition.

III. SECURITY OF QKD AND KEY RATE

This section presents the asymptotic key rate of QKD protocols that employs the IR protocol proposed in Section II. The asymptotic key rate is derived by the security proof method [12, 13, 14].

We implement a prepare and measure scheme in a practical QKD protocol. However, when we analyze the security of a QKD protocol, it is usually more convenient to consider its entanglement-based version. Without compromising security, we can assume that Alice and Bob's raw keys and bit sequences for error estimation are obtained by measuring a bipartite state, $\rho_{A^N B^N}$, on an N pair of bipartite systems $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes N}$, that $\rho_{A^N B^N}$ is invariant under the permutation of the systems [42], and that Eve can access $\mathrm{Tr}_{A^N B^N}[\rho_{A^N B^N E^N}]$ for a purification $\rho_{A^N B^N E^N}$ of $\rho_{A^N B^N}$ (see also [12, 13]). The specific form of $\rho_{A^N B^N}$ depends on which scheme Alice and Bob employ to transmit a binary sequence, noise in the channel, and Eve's attack. From [14, Lemma 4.2.2], without loss of generality, we can assume that purification $\rho_{A^N B^N E^N}$ lies on the symmetric subspace of $(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)^{\otimes N}$, because any purification can be transformed into another purification using Eve's local operation.

Before the protocol is started, Alice and Bob discard the last k subsystems, $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B^{\otimes k}$, for technical reasons of security proof. More specifically, k subsystems are discarded to apply the de Finetti style representation theorem [14, Theorem 4.3.2] (see also [30]) in the security proof. Therefore, we set $N := 2n + m + k$.

Then, Alice and Bob conduct the protocol for the state, $\rho_{A^{2n+m}B^{2n+m}} := \mathrm{Tr}_k[\rho_{A^NB^N}]$, where k is the number of discarded systems, m is the number of systems for parameter estimation, and $2n$ is the number of systems that are used for key distillation.

First, Alice and Bob undertake the following parameter estimation protocol for the last m-subsystems of the state $\rho_{A^{2n+m}B^{2n+m}}$. The parameter estimation protocol is conducted to estimate the number of discrepancies between Alice and Bob's raw keys, and the amount of information that Eve has gained by eavesdropping.

(i) Alice and Bob carry out a bipartite positive operator valued measurement (POVM), $\mathcal{M} := \{M_a\}_{a\in\mathcal{A}}$, for each system, $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{A}$ is the set of measurement outcomes. The specific form of $\mathcal{M}$ depends on which scheme we use.

(ii) If the type, $P_{\mathbf{a}}$, of the measurement outcomes, $\mathbf{a} = (a_1, \ldots, a_m)$, satisfies $P_{\mathbf{a}} \in \mathcal{Q}$ for a prescribed set, $\mathcal{Q}$, the protocol outputs the type, $Q := P_{\mathbf{a}}$, and Alice and Bob conduct the key distillation protocol according to Q, where the type of sequence $\mathbf{a} = (a_1, \ldots, a_m)$ is the frequency distribution defined by

$$P_{\mathbf{a}}(a) := \frac{|\{i \mid 1 \le i \le m,\ a_i = a\}|}{m} \text{ for } a \in \mathcal{A}$$

(for more details on the type, see [31, Chapter 11]). Otherwise, it outputs "abort".

It is convenient to describe the parameter estimation protocol using a completely positive (CP) map as follows. Let $\mathcal{M}^{\otimes m} := \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathcal{A}^m}$ be a product POVM on $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes m}$, where $M_{\mathbf{a}} = M_{a_1} \otimes \cdots \otimes M_{a_m}$. Then, we can define a CP map, $\mathcal{E}_Q$, by

$$\mathcal{E}_Q : \rho_m \mapsto \sum_{\mathbf{a}\in\mathcal{T}_Q^n(\mathcal{A})} \mathrm{Tr} M_{\mathbf{a}} \rho_m, \tag{1}$$

which maps the density operator to the probability such that the parameter estimation protocol outputs Q, where $\mathcal{T}_Q^m(\mathcal{A})$ is a set of all sequences on $\mathcal{A}^m$ with type Q.

When the output of the parameter estimation protocol is $Q \in \mathcal{Q}$, Alice, Bob, and Eve's tripartite state is given by

$$\rho^Q_{A^{2n}B^{2n}E^N} := \frac{1}{P_{\mathsf{PE}}(Q)} (\mathrm{id}_{A^{2n}B^{2n}} \otimes \mathcal{E}_Q \otimes \mathrm{id}_{E^N})(\rho_{A^{2n+m}B^{2n+m}E^N}),$$

where $P_{\mathsf{PE}}(Q)$ is a probability such that the parameter estimation protocol outputs Q, and id denotes the identity map on each system.

Alice and Bob apply a measurement $\mathcal{M}_{XY} := \{M_x \otimes M_y\}_{(x,y)\in\mathbb{F}_2\times\mathbb{F}_2}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ to the remaining $2n$ systems to obtain classical data (raw keys). Then, Alice and Bob's measurement results, $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n}$, and Eve's available information is described by a $\{ccq\}$-state [43]

$$\rho^Q_{\mathbf{XY}E^N} := (\mathcal{E}_{XY}^{\otimes 2n} \otimes \mathrm{id}_{E^N})(\rho^Q_{A^{2n}B^{2n}E^N}),$$

where we introduce a CP map, $\mathcal{E}_{XY}$, that describes the measurement procedure for convenience.

According to output Q of the parameter estimation protocol, Alice and Bob decide the parameters of the IR protocol: rate $R(Q) := \frac{m}{n}$ of linear code $\mathcal{C}_{n,m}$, numbers $\underline{n}_0(Q)$ and $\overline{n}_0(Q)$ that are used in Step (iv), and rate $R_0(Q) := \frac{m_0}{n_0}$ of linear code $\mathcal{C}_{n_0,m_0}$ for $\underline{n}_0(Q) \le n_0 \le \overline{n}_0(Q)$. Furthermore, Alice and Bob also decide the length, $\ell(Q)$, of the finally distilled key according to Q. According to the determined parameters, a final secure key pair is distilled as follows.

(i) Alice and Bob undertake the two-way IR protocol in Section II, and Alice obtains $\hat{\mathbf{u}}$ and Bob obtains $\tilde{\mathbf{u}}$.

(ii) Alice and Bob carry out a privacy amplification (PA) protocol to distill a key pair (s_A, s_B) such that Eve has little information about it. Alice first randomly chooses a hash function, $f : \mathbb{F}_2^{2n} \to \{0,1\}^{\ell(Q)}$, from a family of two-universal hash functions (refer [14, Definition 5.2.1] for a formal definition of a family of two-universal hash functions), and sends the choice of f to Bob over the public channel. Then, Alice's distilled key is $s_A = f(\hat{\mathbf{u}})$ and Bos's distilled key is $s_B = f(\tilde{\mathbf{u}})$.

The distilled key pair and Eve's available information can be described by a $\{cccq\}$-state, $\rho^Q_{S_AS_BCE^N}$, where classical system C consists of random variables $(\mathbf{T}_1, \hat{\mathbf{T}}_2, \hat{\mathbf{W}}_1)$ that describe the exchanged messages $(\mathbf{t}_1, \hat{\mathbf{t}}_2, \hat{\mathbf{w}}_1)$ in the IR protocol and random variable F that describes the choice of the hash function in the PA protocol. To define the security of the distilled key pair (S_A, S_B), we use the universally composable security definition [32, 33], which is defined by the trace distance between the actual key pair and the ideal key pair. We cannot state security in QKD protocols in the sense that the distilled key pair (S_A, S_B) is secure for a particular output Q of the parameter estimation protocol, because there is a slight possibility that the parameter estimation protocol will not output "abort" even though Eve has so much information. The QKD protocol is said to be ε-secure (in the sense of the average over the outputs of the parameter estimation protocol) if

$$\sum_{Q\in\mathcal{Q}} P_{\mathsf{PE}}(Q) \frac{1}{2} \|\rho^Q_{S_AS_BCE^N} - \rho^{Q,\mathrm{mix}}_{S_AS_B} \otimes \rho_{CE^N}\| \le \varepsilon, \tag{2}$$

where $\rho^{Q,\mathrm{mix}}_{S_AS_B} := \sum_{s\in\mathcal{S}_Q} \frac{1}{|\mathcal{S}_Q|} |s,s\rangle\langle s,s|$ is the uniformly distributed key on the key space $\mathcal{S}_Q := \{0,1\}^{\ell(Q)}$.

To state the relation between the security and the asymptotic key rate of the previously mentioned QKD protocol, define

$$\Gamma(Q) := \{\sigma_{AB} \mid P_A^{\sigma_{AB}} = Q\}$$

as the set of two-qubit density operators that are compatible with output Q of the parameter estimation protocol, where $P_A^{\sigma_{AB}}$ denotes the probability distribution of the outcomes when measuring σ_{AB} with POVM $\mathcal{M}$, i.e., $P_A^{\sigma_{AB}}(a) := \mathrm{Tr}[M_a \sigma_{AB}]$. For a purification, σ_{ABE}, of a density operator, $\sigma_{AB} \in \Gamma(Q)$, let $\sigma_{X_1X_2Y_1Y_2E_1E_2} := (\mathcal{E}_{XY}^{\otimes 2} \otimes \mathrm{id}_E^{\otimes 2})(\sigma_{ABE}^{\otimes 2})$ be a $\{ccq\}$-state that consists of 2-bit pairs $((X_1, X_2), (Y_1, Y_2))$ and environment systems E_1, E_2. By using functions ξ_1 and ξ_2, define random variables (U_1, U_2, W_1, W_2) for the pair of bits $((X_1, X_2), (Y_1, Y_2))$ in the same way as in Section II. Then, let $\sigma_{U_1U_2W_1E_1E_2}$ and $\sigma_{U_1U_2W_1U_1E_1E_2}$ be density operators that respectively describe the classical random variables (U_1, U_2, W_1) and (U_1, U_2, W_1, U_1) with the environment system E_1, E_2.

Theorem 2 For $Q \in \mathcal{Q}$, i.e., the output of the parameter estimation protocol such that the QKD protocol does not abort, let $\frac{\ell(Q)}{2n}$ be the key rate of the protocol. For any $\varepsilon > 0$, if the key rate satisfies

$$\begin{aligned}\frac{\ell(Q)}{2n} \;<\; & \frac{1}{2} \min_{\sigma_{AB} \in \Gamma(Q)} \max\Big[H_\sigma(U_1U_2|W_1E_1E_2) \\ & -H(P_{W_1}) - P_{W_1}(0) H(P_{W_2|W_1=0}), \\ & H_\sigma(U_2|W_1U_1E_1E_2) - P_{W_1}(0) H(P_{W_2|W_1=0}) \Big],\end{aligned} \tag{3}$$

then there exists a protocol that is ε-secure in the sense of Eq. (2) for sufficiently large n, where $H_\rho(A|B) := H(\rho_{AB}) - H(\rho_B)$ is conditional von Neumann entropy [34], and $H(P)$ is Shannon entropy [31].

The meaning of the two arguments of the maximum in Eq. (3) should be noted. The first argument states that the key rate is given by the difference between Eve's ambiguity, $H_\sigma(U_1U_2|W_1E_1E_2)$, about Alice's reconciled key and the amount, $H(P_{W_1}) + P_{W_1}(0)H(P_{W_2|W_1=0})$, of information leaked in the IR protocol. On the other hand, since information leaked from the syndrome, $\mathbf{t}_1 = \mathbf{u}_1 M_{\mathcal{C}_{n,m}}^T$, cannot be more than $\mathbf{u}_1$ itself, we can evaluate the key rate under the condition that Eve can access $\mathbf{u}_1$ itself, i.e., Eve's ambiguity, $H_\sigma(U_2|W_1U_1E_1E_2)$, about Alice's reconcilied key and the amount, $P_{W_1}(0)H(P_{W_2|W_1=0})$, of information leaked in the IR protocol. If either of them is omitted, the key rate is underestimated, which will be discussed in Section IV.

Theorem 2 is formally proved by demonstrating the above intuition formally, where we use a security proof method [12, 13, 14]. More precisely, we use the techniques of privacy amplification and minimum entropy, and the de Finetti style representation theorem and the property of symmetric states (see [14]). Since the techniques used in the proof are not new and involved, we give the proof for Theorem 2 in the Appendix.

IV. ANALYSIS OF KEY RATE

Here, we analyze the asymptotic key rate formula in Theorem 2. More precisely, we derive a specific form of the key rate formulas as functions of the error rates for the six-state [4] and BB84 protocols [3].

Before analyzing the key rate, let us define some notations. For $\mathsf{x}, \mathsf{z} \in \mathbb{F}_2$, let

$$|\psi(\mathsf{x},\mathsf{z})\rangle := \frac{1}{\sqrt{2}}(|0\rangle|0+\mathsf{x}\rangle + (-1)^{\mathsf{z}}|1\rangle|1+\mathsf{x}\rangle)$$

be the Bell states on two-qubit systems $\mathcal{H}_A \otimes \mathcal{H}_B$. For a probability distribution, P_{XZ}, on $\mathbb{F}_2 \times \mathbb{F}_2$, a state of the form,

$$\sum_{\mathsf{x},\mathsf{z} \in \mathbb{F}_2} P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z}) |\psi(\mathsf{x},\mathsf{z})\rangle\langle\psi(\mathsf{x},\mathsf{z})|,$$

is called a Bell diagonal state. We occasionally abbreviate $P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z})$ as p_{xz}.

Theorem 3 For a Bell diagonal state, $\sigma_{AB} = \sum_{\mathsf{x},\mathsf{z} \in \mathbb{F}_2} P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z}) |\psi(\mathsf{x},\mathsf{z})\rangle\langle\psi(\mathsf{x},\mathsf{z})|$, we have

$$\begin{aligned}&\frac{1}{2}\max[H_\sigma(U_1U_2|W_1E_1E_2) \\ &\quad -H(P_{W_1}) - P_{W_1}(0)H(P_{W_2|W_1=0}), \\ &\quad H_\sigma(U_2|W_1U_1E_1E_2) - P_{W_1}(0)H(P_{W_2|W_1=0})] \\ &= \max[1 - H(P_{\mathsf{XZ}}) \\ &\quad + \frac{P_{\bar{\mathsf{X}}}(1)}{2} h\left(\frac{p_{00}p_{10} + p_{01}p_{11}}{(p_{00}+p_{01})(p_{10}+p_{11})}\right), \\ &\quad \frac{P_{\bar{\mathsf{X}}}(0)}{2}(1 - H(P'_{\mathsf{XZ}}))],\end{aligned} \tag{4}$$

where $h(p) := -p\log p - (1-p)\log(1-p)$ is the binary entropy function,

$$\begin{aligned}P_{\bar{\mathsf{X}}}(0) &:= (p_{00}+p_{01})^2 + (p_{10}+p_{11})^2, \\ P_{\bar{\mathsf{X}}}(1) &:= 2(p_{00}+p_{01})(p_{10}+p_{11}),\end{aligned}$$

and

$$\begin{aligned}P'_{\mathsf{XZ}}(0,0) &:= \frac{p_{00}^2 + p_{01}^2}{(p_{00}+p_{01})^2 + (p_{10}+p_{11})^2}, \\ P'_{\mathsf{XZ}}(1,0) &:= \frac{2p_{00}p_{01}}{(p_{00}+p_{01})^2 + (p_{10}+p_{11})^2}, \\ P'_{\mathsf{XZ}}(0,1) &:= \frac{p_{10}^2 + p_{11}^2}{(p_{00}+p_{01})^2 + (p_{10}+p_{11})^2}, \\ P'_{\mathsf{XZ}}(1,1) &:= \frac{2p_{10}p_{11}}{(p_{00}+p_{01})^2 + (p_{10}+p_{11})^2}.\end{aligned}$$

The theorem is proved by a straight forward calculation. Thus, the proof is presented in the Appendix E.

The six-state protocol [4] uses three different bases defined by z-basis $\{|0_z\rangle, |1_z\rangle\}$, x-basis $\{1/\sqrt{2}(|0_z\rangle \pm |1_z\rangle)\}$, and y-basis $\{1/\sqrt{2}(|0_z\rangle \pm i|1_z\rangle)\}$. When Alice and Bob

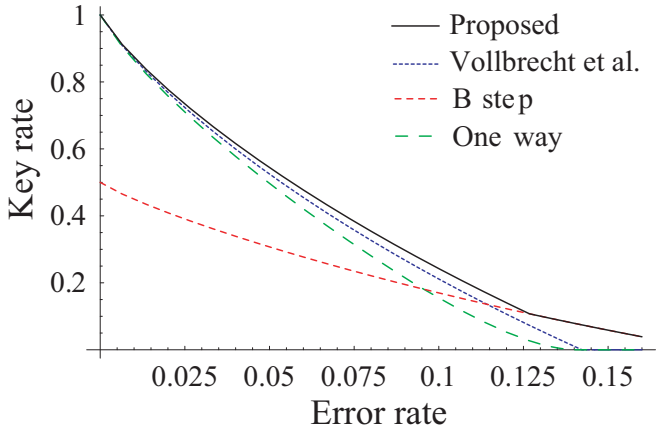

FIG. 1: (Color online) Comparison of the key rates of the six-state protocols. "Proposed" is the key rate of the six-state protocol that uses the proposed IR protocol. "Vollbrecht et al." is the key rate of the two-way six-state protocol of [17, 24]. "B-step" is the key rate of the two-way six-state protocol of [15]. "One-way" is the key rate of the one-way six-state protocol with the noisy preprocessing [13]. It should be noted that the key rates of two-way six-state protocols of [14, 15, 16] are slightly higher than that of the proposed protocol for much higher error rate.

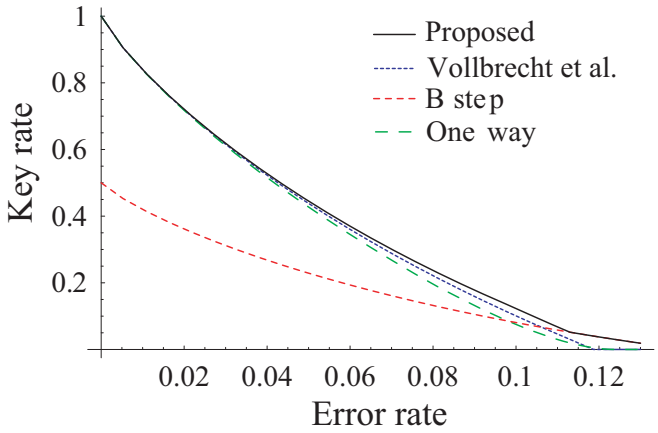

FIG. 2: (Color online) Comparison of the key rates of the BB84 protocols. "Proposed" is the key rate of the BB84 protocol that uses the proposed IR protocol. "Vollbrecht et al." is the key rate of the two-way BB84 protocol of [17, 24]. "B-step" is the key rate of the two-way BB84 protocol of [15]. "One-way" is the key rate of the one-way BB84 protocol with the noisy preprocessing [13].

obtain an error rate, e, the set $\Gamma(Q)$ consists of states whose Bell diagonal entries $p_{00}, p_{10}, p_{01}, p_{11}$ satisfy conditions $p_{10}+p_{11}=e$, $p_{01}+p_{11}=e$, and $p_{01}+p_{10}=e$. Together with the normalization condition, we find $p_{00}=1-\frac{3e}{2}$ and $p_{10}=p_{01}=p_{11}=\frac{e}{2}$. Since it is sufficient only to minimize over the Bell diagonal states (see the Appendix F), the key rate of the six-state protocol for the error rate e is given by substituting $p_{00}=1-\frac{3e}{2}$ and $p_{10}=p_{01}=p_{11}=\frac{e}{2}$ into Eq. (4). The key rate of the six-state protocol that uses the proposed IR protocol is plotted in Fig. 1.

The BB84 protocol is similar to the six-state protocol, but only uses the z-basis and the x-basis to transmit a bit sequence. Thus, we only obtain two conditions on the four coefficients $p_{00}, p_{10}, p_{01}, p_{11}$. Thus, the set $\Gamma(Q)$ consists of states whose Bell diagonal entries satisfy conditions $p_{10}+p_{11}=e$ and $p_{01}+p_{11}=e$. The resulting candidates for Bell diagonal states in $\Gamma(Q)$ have coefficients $p_{00}=1-2e+p_{11}$, $p_{10}=p_{01}=e-p_{11}$, and $p_{11}\in[0,e]$, and we have to minimize the key rate formula of Eq. (4) over the free parameter, $p_{11}\in[0,e]$. The key rate of the BB84 protocol that uses the proposed IR protocol is plotted in Fig. 2.

Remark 4 By using the chain rule of von Neumann entropy, we can rewrite the l.h.s. of Eq. (4) as

$$\frac{1}{2}\{\max[H_\sigma(U_1|W_1E_1E_2)-H(P_{W_1}),0] + H_\sigma(U_2|W_1U_1E_1E_2)-P_{W_1}(0)H(P_{W_2|W_1=0})\}. \quad (5)$$

We can interpret this formula as follows. If Bob's ambiguity, $H(P_{W_1})$, about bit U_1, i.e., the amount of transmitted syndrome per bit, is smaller than Eve's ambiguity, $H_\sigma(U_1|W_1E_1E_2)$, about bit U_1, then Eve cannot decode sequence $\mathbf{U}_1$ [35, 36], and there exists some remaining ambiguity about bit U_1 for Eve. We can thus distill some secure key from bit U_1. On the other hand, if Bob's ambiguity, $H(P_{W_1})$, about bit U_1, i.e., the amount of transmitted syndrome per bit, is larger than Eve's ambiguity, $H_\sigma(U_1|W_1E_1E_2)$, about U_1, then Eve might be able to decode sequence $\mathbf{U}_1$ from her side information, W_1, E_1, E_2, and the transmitted syndrome [35, 36]. Thus, there exists the possibility that Eve can completely know bit U_1, and we can distill no secure key from bit U_1, because we have to consider the worst case in a cryptographic scenario. Consequently, sending the hashed version (syndrome) of sequence $\mathbf{U}_1$ instead of $\mathbf{U}_1$ itself is not always effective, and the slopes of the key rate curves in Figs. 1 and 2 change when Eve becomes able to decode $\mathbf{U}_1$.

The second and third terms of Eq. (5) are the same as the key rate formula of the protocol that uses Gottesman and Lo's B-step [15] followed by error correction and privacy amplification. Even though Alice sends the sequence $\mathbf{U}_1$ itself instead of its hashed version in the B-step, the key rate of the protocol with the B-step is equal to that of the proposed protocol for high error rates, because Eve can decode sequence $\mathbf{U}_1$ from her side information and the transmitted syndrome.

Remark 5 The yield of Vollbrecht and Vestraete's EDP [22] and the key rate of the QKD protocols [17, 24] are given by

$$1-H(P_{\mathsf{XZ}}) + \frac{P_{\mathsf{X}}(1)}{4}\left\{h\left(\frac{p_{01}}{p_{00}+p_{01}}\right)+h\left(\frac{p_{11}}{p_{10}+p_{11}}\right)\right\}. \quad (6)$$

We can find by the concavity of the binary entropy function that the first argument in the maximum of the r.h.s. of Eq. (4) is larger than the value in Eq. (6). To explain why the key rate of the proposed protocol is higher than that of [17, 24], we need to review the EDP [22] by using the notations in Section II. Assume that Alice and Bob share Bell diagonal states, $\sigma_{AB}^{\otimes 2n}$. First, Alice and Bob divide $2n$ pairs into n blocks of length 2, and locally carry out CNOT operation on each block, where the $2i$-th pair is the source and $(2i-1)$-th pair is the target. Then, Alice and Bob undertake the breeding protocol [9] to guess bit flip errors in the $(2i-1)$-th pair for all i. The guessed bit flip errors can be described by a sequence, $\hat{\mathbf{w}}_1$. Note that two-way communication is used in this step. According to sequence $\hat{\mathbf{w}}_1$, Alice and Bob classify indices of blocks into two sets, $\hat{\mathsf{T}}_0$ and $\hat{\mathsf{T}}_1$. For a collection of $2i$-th pairs such that $i \in \hat{\mathsf{T}}_0$, Alice and Bob conduct the breeding protocol to correct bit flip errors. For a collection of $2i$-th pairs such that $i \in \hat{\mathsf{T}}_1$, Alice and Bob perform measurements by $\{|0_z\rangle, |1_z\rangle\}$ basis, and obtain measurement results, $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ and $\mathbf{y}_{2,\hat{\mathsf{T}}_1}$. Alice sends $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ to Bob. Alice and Bob correct the phase errors for the remaining pairs by using information $\hat{\mathsf{T}}_0$ and $\hat{\mathsf{T}}_1$, and bit flip error $\mathbf{x}_{2,\hat{\mathsf{T}}_1} + \mathbf{y}_{2,\hat{\mathsf{T}}_1}$.

If we convert this EDP into a QKD protocol, the difference between that QKD protocol and ours is as follows. In the protocol converted from [22], after Step (iii), Alice reveals the sequence, $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$, which consists of the second bit, x_{i2}, of the i-th block such that the parity of discrepancies $\hat{w}_{i1}$ is 1. However, Alice discards $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ in the proposed IR protocol of Section II. Since sequence $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ has some correlation to sequence $\mathbf{u}_1$ from the view point of Eve, Alice should not reveal $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ to achieve a higher key rate.

In the EDP context, on the other hand, since the bit flip error, $\mathbf{x}_{2,\hat{\mathsf{T}}_1} + \mathbf{y}_{2,\hat{\mathsf{T}}_1}$, has some correlation to the phase flip errors in the $(2i-1)$-th pair with $i \in \hat{\mathsf{T}}_1$, Alice should send the measurement results, $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$, to Bob. If Alice discards measurement results $\mathbf{x}_{2,\hat{\mathsf{T}}_1}$ without telling Bob what the result is, then the yield of the resulting EDP is worse than Eq. (6). Consequently, there seems to be no correspondence between the EDP and our proposed classical processing.

V. CONCLUSION

We proposed an information reconciliation protocol that uses two-way classical communication. For the BB84 and six-state protocols, the key rates of QKD protocols that uses our information reconciliation protocol are higher than previously known protocols for a wide range of error rates. Furthermore, we showed the relation between the proposed protocol and the B-step of [15] (Remark 4). We clarified why the key rate of our protocol is higher than those of [17, 22, 24] (Remark 5), and found that there does not seem to be any EDP that corresponds to our proposed QKD protocol.

Acknowledgment

The first author partly contributed to this work during his internship at Nippon Telegraph Communication Science Laboratories. This research was also partly supported by the Japan Society for the Promotion of Science under a Grants-in-Aid for Young Scientists, No. 18760266, and a Grants-in-Aid for JSPS Fellows.

APPENDIX A: NOTATIONS

These appendices are suplementary materials, in which we prove Theorem 2, Theorem 3, and the fact that the key rate formula evaluated for a Bell-diagonal state is the worst case. The proof of Theorem 2 is based on the proof method of [12, 13, 14], especially [14]. In Section A, we review notations and fundamental results that are used in subsequent sections. Notations in this paper is almost the same as those in [14]. In Section B, we review notions of the (smooth) min-entropy, the (smooth) max-entropy, and the privacy amplification. Furthermore, we additionally show some lemmas, which are used to prove Theorem 2 in Section D. In Section C, we review the property of symmetric states and the de Finetti style representation theorem [14, 30]. We prove Theorem 2 in Section D. Section E presents a proof of Theorem 3. We show the fact that the key rate formula evaluated for a Bell-diagonal state is the worst case in Section F.

1. Fundamentals

For a finite set $\mathcal{X}$, let $\mathcal{P}(\mathcal{X})$ be the set of non-negative functions P on $\mathcal{X}$, i.e., $P(x) \geq 0$ for all $x \in \mathcal{X}$. If $P \in \mathcal{P}(\mathcal{X})$ is normalized, i.e., $\sum_{x\in\mathcal{X}} P(x) = 1$, then P is a probability distribution on $\mathcal{X}$. Unless stated as a probability distribution, $P \in \mathcal{P}(\mathcal{X})$ is not necessarily normalized.

For a finite-dimensional Hilbert space $\mathcal{H}$, let $\mathcal{P}(\mathcal{H})$ be the set of non-negative operator ρ on $\mathcal{H}$. If $\rho \in \mathcal{P}(\mathcal{H})$ is normalized, i.e., $\mathrm{Tr}\rho = 1$, then ρ is called a density operator. Mathematically, a state of a quantum mechanical system with d-degree of freedom is represented by a density operator on $\mathcal{H}$ with $\dim \mathcal{H} = d$. Unless stated as a density operator or a state, $\rho \in \mathcal{P}(\mathcal{H})$ is not necessarily normalized. For Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the set of non-negative operators $\mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ on the tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined in a similar manner.

The classical random variables can be regarded as a special case of the quantum states. For a random variable X with a distribution $P_X \in \mathcal{P}(\mathcal{X})$, let

$$\rho_X := \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x|,$$

where $\{|x\rangle\}_{x\in\mathcal{X}}$ is an orthonormal basis of $\mathcal{H}_X$. We call ρ_X the operator representation of the classical distribution P_X.

When a quantum system $\mathcal{H}_A$ is prepared in a state ρ_A^x according to a realization x of a random variable X with a probability distribution P_X, it is convenient to denote it by a density operator

$$\rho_{XA} := \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_A^x \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_A), \quad \text{(A1)}$$

where $\{|x\rangle\}_{x\in\mathcal{X}}$ is an orthonormal basis of $\mathcal{H}_X$. We call the density operator ρ_{XA} a $\{cq\}$-state [37], or we say ρ_{XA} is classical on $\mathcal{H}_X$. We call ρ_A^x a conditional operator. When a quantum system $\mathcal{H}_A$ is prepared in a state $\rho_A^{x,y}$ according to a joint random variable (X,Y) with a probability distribution P_{XY}, a state ρ_{XYA} is defined in a similar manner, and the state ρ_{XYA} is called a $\{ccq\}$-state.

In quantum mechanics, the most general state evolution of a quantum mechanical system is described by a completely positive (CP) map. It can be shown that any CP map $\mathcal{E}$ can be written as

$$\mathcal{E}(\rho) = \sum_{a\in\mathcal{A}} E_a \rho E_a^* \quad \text{(A2)}$$

for a family of linear operators $\{E_a\}_{a\in\mathcal{A}}$ from the initial system $\mathcal{H}$ to the destination system $\mathcal{H}'$. We usually require the map to be trace preserving (TP), i.e., $\sum_{a\in\mathcal{A}} E_a^* E_a = \mathrm{id}_{\mathcal{H}}$, but if a state evolution involves a measurement, then the corresponding CP map is not necessarily trace preserving, i.e., $\sum_{a\in\mathcal{A}} E_a^* E_a \le \mathrm{id}_{\mathcal{H}}$.

2. Distance and fidelity

In this paper, we use two kind of distances. One is the variational distance of $\mathcal{P}(\mathcal{X})$. For non-negative functions $P, P' \in \mathcal{P}(\mathcal{X})$, the variational distance between P and P' is defined by

$$\|P - P'\| := \sum_{x\in\mathcal{X}} |P(x) - P'(x)|.$$

The other distance used in this paper is the trace distance of $\mathcal{P}(\mathcal{H})$. For nen-negative operators $\rho, \sigma \in \mathcal{P}(\mathcal{H})$, the trace distance between ρ and σ is defined by

$$\|\rho - \sigma\| := \mathrm{Tr}|\rho - \sigma|,$$

where $|A| := \sqrt{A^*A}$ for a operator on $\mathcal{H}$, and A^* is the adjoint operator of A. The following lemma states that the trace distance between (not necessarily normalized operators) does not increase by applying a CP map, and it is used several times in this paper.

Lemma 6 [14, Lemma A.2.1] Let $\rho, \rho' \in \mathcal{P}(\mathcal{H})$ and let $\mathcal{E}$ be a trace-non-increasing CP map, i.e., $\mathcal{E}$ satisfies $\mathrm{Tr}\mathcal{E}(\sigma) \le \mathrm{Tr}\sigma$ for any $\sigma \in \mathcal{P}(\mathcal{H})$. Then we have

$$\|\mathcal{E}(\rho) - \mathcal{E}(\rho')\| \le \|\rho - \rho'\|.$$

The following lemma states that, for a $\{cq\}$-state ρ_{XB}, if two classical messages v and $\bar{v}$ are computed from x and they are equal with high probability, then the $\{ccq\}$ state ρ_{XVB} and $\rho_{X\bar{V}B}$ that involve computed classical messages v and $\bar{v}$ are close with respect to the trace distance.

Lemma 7 Let

$$\rho_{XB} := \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_B^x$$

be a $\{cq\}$-state, and let $V := f(X)$ for a function f and $\bar{V} := g(X)$ for a function g. Assume that

$$\Pr\{V \neq \overline{V}\} = \sum_{\substack{x\in\mathcal{X} \\ f(x)\neq g(x)}} P_X(x) \le \varepsilon.$$

Then, for $\{ccq\}$-states

$$\rho_{XVB} := \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes |f(x)\rangle\langle f(x)| \otimes \rho_B^x$$

and

$$\rho_{X\overline{V}B} := \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes |g(x)\rangle\langle g(x)| \otimes \rho_B^x,$$

we have

$$\|\rho_{XVB} - \rho_{X\overline{V}B}\| \le 2\varepsilon.$$

Proof. We have

$$\begin{aligned} & \|\rho_{XVB} - \rho_{X\overline{V}B}\| \\ = & \sum_{x\in\mathcal{X}} P_X(x) \| |x\rangle\langle x| \| \\ & \quad \cdot \| |f(x)\rangle\langle f(x)| - |g(x)\rangle\langle g(x)| \| \cdot \|\rho_B^x\| \\ = & \sum_{x\in\mathcal{X}} P_X(x) \cdot 2(1 - \delta_{f(x),g(x)}) \\ \le & \ 2\varepsilon, \end{aligned}$$

where $\delta_{a,b} = 1$ if $a = b$ and $\delta_{a,b} = 0$ if $a \neq b$. □

The fidelity between two (not necessarily normalized) operators $\rho, \sigma \in \mathcal{P}(\mathcal{H})$ is defined by

$$F(\rho,\sigma) := \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}.$$

The following lemma is an extension of Uhlmann's theorem to non-normalized operators ρ and σ.

Lemma 8 [14, Theorem A.1.2] Let $\rho, \sigma \in \mathcal{P}(\mathcal{H})$, and let $|\psi\rangle \in \mathcal{H}_R \otimes \mathcal{H}$ be a purification of ρ. Then

$$F(\rho,\sigma) = \max_{|\phi\rangle\langle\phi|} F(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|),$$

where the maximum is taken over all purifications $|\phi\rangle \in \mathcal{H}_R \otimes \mathcal{H}$ of σ.

The trace distance and the fidelity have close relationship. If the trace distance between two density operators ρ and σ is close to 0, then the fidelity between ρ and σ is close to 1, and vise versa.

Lemma 9 [14, Lemma A.2.4] Let $\rho, \sigma \in \mathcal{P}(\mathcal{H})$. Then, we have

$$\|\rho - \sigma\| \leq \sqrt{(\mathrm{Tr}\rho + \mathrm{Tr}\sigma)^2 - 4F(\rho,\sigma)^2}.$$

Lemma 10 [14, Lemma A.2.6] Let $\rho, \sigma \in \mathcal{P}(\mathcal{H})$. Then, we have

$$\mathrm{Tr}\rho + \mathrm{Tr}\sigma - 2F(\rho,\sigma) \leq \|\rho - \sigma\|.$$

3. Entropy

For a random variable X on $\mathcal{X}$ with a probability distribution $P_X \in \mathcal{P}(\mathcal{X})$, the entropy of X is defined by

$$H(X) = H(P_X) := -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x),$$

where the base of log is 2. Especially for a real number $0 \leq p \leq 1$, the binary entropy function is defined by

$$h(p) := -p\log p - (1-p)\log(1-p).$$

Similarly, for a joint random variables X and Y with a joint probability distribution $P_{XY} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$, the joint entropy of X and Y is

$$\begin{aligned} H(XY) &= H(P_{XY}) \\ &:= -\sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P_{XY}(x,y)\log P_{XY}(x,y). \end{aligned}$$

The conditional entropy of X given Y is defined by

$$H(X|Y) := H(XY) - H(Y).$$

For a quantum state $\rho \in \mathcal{P}(\mathcal{H})$, the von Neumann entropy of the system is defined by

$$H(\rho) := \mathrm{Tr}\rho\log\rho.$$

For a quantum state $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ of the composite system, the von Neumann entropy of the composite system is $H(\rho_{AB})$. The conditional von Neaumann entropy of the system A given the system B is defined by

$$H_\rho(A|B) := H(\rho_{AB}) - H(\rho_B),$$

where $\rho_B = \mathrm{Tr}_A[\rho_{AB}]$ is the partial trace of ρ_{AB} over the system A.

Remark 11 In this paper, we denote ρ_A for $\mathrm{Tr}_B[\rho_{AB}]$ or ρ_B for $\mathrm{Tr}_{AC}[\rho_{ABC}]$ e.t.c. without declaring them if they are obvious from the context.

4. Method of type

In this section, we review the method of type that are used in this paper (see [31, Chapter 11] for more detail).

For a sequence $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{X}^n$, the type of $\mathbf{x}$ is the empirical probability distribution $P_\mathbf{x} \in \mathcal{P}(\mathcal{X})$ defined by

$$P_\mathbf{x}(a) := \frac{|\{i \mid x_i = a\}|}{n} \qquad \text{for } a \in \mathcal{X},$$

where $|A|$ is the cardinality of a set A. Let

$$\mathcal{P}_n(\mathcal{X}) := \{P_\mathbf{x} \mid \mathbf{x} \in \mathcal{X}^n\}$$

be the set of all types on $\mathcal{X}^n$. It is easy to confirm that

$$|\mathcal{P}_n(\mathcal{X})| \leq (n+1)^{(|\mathcal{X}|-1)}.$$

For $Q \in \mathcal{P}_n(\mathcal{X})$,

$$\mathcal{T}_Q^n(\mathcal{X}) := \{\mathbf{x} \in \mathcal{X}^n \mid P_\mathbf{x} = Q\}$$

is the set of all sequences of type Q.

The probability that sequences in the set $\mathcal{T}_Q^n$ occur can be expressed in terms of the divergence.

Lemma 12 [31, Theorem 11.1.4] For any probability distribution $P \in \mathcal{P}(\mathcal{X})$ and for any type $Q \in \mathcal{P}_n(\mathcal{X})$, we have

$$\begin{aligned} \frac{1}{(n+1)^{(|\mathcal{X}|-1)}}\exp\{-nD(Q\|P)\} \;&\leq\; P^n(\mathcal{T}_Q^n) \\ &\leq\; \exp\{-nD(Q\|P)\}, \end{aligned}$$

where $P^n(\mathcal{T}_Q^n) := \sum_{\mathbf{x}\in\mathcal{T}_Q^n} P^n(\mathbf{x})$, the base of $\exp\{\}$ is 2, and $D(Q\|P)$ is the divergence defined by

$$D(Q\|P) := \sum_{x\in\mathcal{X}} Q(x)\log\frac{Q(x)}{P(x)}.$$

In the subsequent sections, we especially use the following inequality:

$$Q^n(\mathcal{T}_Q^n(\mathcal{X})) \geq \frac{1}{(n+1)^{(|\mathcal{X}|-1)}} \tag{A3}$$

for any $Q \in \mathcal{P}_n(\mathcal{X})$, which follows from the fact that $D(Q\|Q) = 0$.

Lemma 13 [31, Lemma 11.6.1] For any probability distributions $P, P' \in \mathcal{P}(\mathcal{X})$, we have

$$D(P\|P') \geq \frac{1}{2\ln 2}\|P - P'\|^2.$$

The following corollary states that sequences whose types are not close to P rarely occur as n increases.

Corollary 14 For any probability distribution $P \in \mathcal{P}(\mathcal{X})$ and a set $\mathcal{B}^\varepsilon(P) := \{\mathbf{x} \in \mathcal{X}^n \mid \|P_\mathbf{x} - P\| \leq \varepsilon\}$, we have

$$\sum_{\mathbf{x}\notin\mathcal{B}^\varepsilon(P)} P^n(\mathbf{x}) \leq (n+1)^{(|\mathcal{X}|-1)}\exp\left\{-\frac{\varepsilon^2 n}{2\ln 2}\right\}.$$

APPENDIX B: PRIVACY AMPLIFICATION

In this section, we review the privacy amplification. First, we review notions of the (smooth) min-entropy and the (smooth) max-entropy. The (smooth) min-entropy and the (smooth) max-entropy are useful tool to prove the security of QKD protocol [12, 13, 14]. Especially, (smooth) min-entropy is much more important, because it is related to the length of the securely distillable key by the privacy amplification. The privacy amplification [2] is a technique to distill a secret key from partially secret data, on which an adversary might have some information. Later, the privacy amplification was extended to the case that an adversary have information encoded into a state of a quantum system [14, 33, 38, 39]). Most of the following results can be found in [14, Sections 3 and 5], but lemmas without citations are additionally proved in this paper. We need Lemma 22 to apply the results in [14] to our proposed two-way QKD protocol (QKD protocol with our proposed IR protocol). More specifically, Eq. (3.22) in [14, Theorem 3.2.12] plays an important role to show a statement similar as Corollary 23 in the case of one-way QKD protocol (QKD protocol with one-way IR protocol). However, the condition of Eq. (3.22) in [14, Theorem 3.2.12] is too restricted, and cannot be applied to our protocol. Thus, we showed Corollary 23 via Lemma 22. Lemmas 19 and 21 are needed to prove Lemma 22. Lemmas 25–28 are implicitly used in [14] without proof, which are also used in our proof in Section D.

1. Min- and Max- Entropy

The (smooth) min-entropy and (smooth) max-entropy are formally defined as follows.

Definition 15 [14, Definition 3.1.1] Let $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$. The min-entropy of ρ_{AB} relative to σ_B is defined by

$$H_{\min}(\rho_{AB}|\sigma_B) := -\log \lambda,$$

where λ is the minimum real number such that $\lambda \cdot \mathrm{id}_A \otimes \sigma_B - \rho_{AB} \geq 0$, where id_A is the identity operator on $\mathcal{H}_A$. When the condition $\mathrm{supp}(\rho_B) \subset \mathrm{supp}(\sigma_B)$ does not hold, there is no λ satisfying the condition $\lambda \cdot \mathrm{id}_A \otimes \sigma_B - \rho_{AB} \geq 0$, thus we define $H_{\min}(\rho_{AB}|\sigma_B) := -\infty$.

The max-entropy of ρ_{AB} relative to σ_B is defined by

$$H_{\max}(\rho_{AB}|\sigma_B) := \log \mathrm{Tr}\left((\mathrm{id}_A \otimes \sigma_B)\rho_{AB}^0\right),$$

where ρ_{AB}^0 denotes the projector onto the support of ρ_{AB}.

The min-entropy and the max-entropy of ρ_{AB} given $\mathcal{H}_B$ are defined by

$$\begin{aligned} H_{\min}(\rho_{AB}|B) &:= \sup_{\sigma_B} H_{\min}(\rho_{AB}|\sigma_B) \\ H_{\max}(\rho_{AB}|B) &:= \sup_{\sigma_B} H_{\max}(\rho_{AB}|\sigma_B), \end{aligned}$$

where the supremum ranges over all $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$ with $\mathrm{Tr}\sigma_B = 1$.

When $\mathcal{H}_B$ is the trivial space $\mathbb{C}$, the min-entropy and the max-entropy of ρ_A is

$$\begin{aligned} H_{\min}(\rho_A) &= -\log \lambda_{\max}(\rho_A) \\ H_{\max}(\rho_A) &= \log \mathrm{rank}(\rho_A), \end{aligned}$$

where $\lambda_{\max}(\cdot)$ denotes the maximum eigenvalue of the argument.

Definition 16 [14, Definitions 3.2.1 and 3.2.2] Let $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$, $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$, and $\varepsilon \geq 0$. The ε-smooth min-entropy and the ε-smooth max-entropy of ρ_{AB} relative to σ_B are defined by

$$\begin{aligned} H_{\min}^{\varepsilon}(\rho_{AB}|\sigma_B) &:= \sup_{\overline{\rho}_{AB}} H_{\min}(\overline{\rho}_{AB}|\sigma_B) \\ H_{\max}^{\varepsilon}(\rho_{AB}|\sigma_B) &:= \inf_{\overline{\rho}_{AB}} H_{\max}(\overline{\rho}_{AB}|\sigma_B), \end{aligned}$$

where the supremum and infimum ranges over the set $\mathcal{B}^{\varepsilon}(\rho_{AB})$ of all operators $\overline{\rho}_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ such that $\|\overline{\rho}_{AB} - \rho_{AB}\| \leq (\mathrm{Tr}\rho_{AB})\varepsilon$.

The conditional ε-smooth min-entropy and the ε-smooth max-entropy of ρ_{AB} given $\mathcal{H}_B$ are defined by

$$\begin{aligned} H_{\min}^{\varepsilon}(\rho_{AB}|B) &:= \sup_{\sigma_B} H_{\min}^{\varepsilon}(\rho_{AB}|\sigma_B) \\ H_{\max}^{\varepsilon}(\rho_{AB}|B) &:= \sup_{\sigma_B} H_{\max}^{\varepsilon}(\rho_{AB}|\sigma_B), \end{aligned}$$

where the supremum ranges over all $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$ with $\mathrm{Tr}\sigma_B = 1$.

The following lemma is a kind of chain rule for the smooth Min-entropy.

Lemma 17 [14, Theorem 3.2.12] For a tripartite operator $\rho_{ABC} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, we have

$$H_{\min}^{\varepsilon}(\rho_{ABC}|C) \leq H_{\min}^{\varepsilon}(\rho_{ABC}|BC) + H_{\max}(\rho_B). \quad \text{(B1)}$$

The following lemma states that removing the classical system only decreases the Min-entropy.

Lemma 18 [14, Lemma 3.1.9] (monotonicity of min-entropy) Let $\rho_{XBC} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ be classical on $\mathcal{H}_X$, and let $\sigma_C \in \mathcal{P}(\mathcal{H}_C)$. Then, we have

$$H_{\min}(\rho_{XBC}|\sigma_C) \geq H_{\min}(\rho_{BC}|\sigma_C).$$

In order to extend Lemma 18 to the smooth min-entropy, we need Lemmas 19 and 21.

Lemma 19 Let $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a density operator. For $\varepsilon \geq 0$, let $\hat{\rho}_B \in \mathcal{B}^{\varepsilon}(\rho_B)$. Then, there exists a operator $\hat{\rho}_{AB} \in \mathcal{B}^{\bar{\varepsilon}}(\rho_{AB})$ such that $\mathrm{Tr}_A[\hat{\rho}_{AB}] = \hat{\rho}_B$, where $\bar{\varepsilon} := \sqrt{8\varepsilon}$.

Proof. Since $\hat{\rho}_B \in \mathcal{B}^\varepsilon(\rho_B)$, we have

$$\|\hat{\rho}_B\| \geq \|\rho_B\| - \|\rho_B - \hat{\rho}_B\| \geq 1 - \varepsilon.$$

Then, from Lemma 10, we have

$$\begin{aligned} F(\rho_B, \hat{\rho}_B) &\geq \frac{1}{2}(\mathrm{Tr}\rho_B + \mathrm{Tr}\hat{\rho}_B - \|\rho_B - \hat{\rho}_B\|) \\ &\geq 1 - \varepsilon. \end{aligned}$$

Let $|\Psi\rangle \in \mathcal{H}_R \otimes \mathcal{H}_A \otimes \mathcal{H}_B$ be a purification of ρ_{AB}. Then, from Theorem 8, there exists a purification $|\Phi\rangle \in \mathcal{H}_R \otimes \mathcal{H}_A \otimes \mathcal{H}_B$ of $\hat{\rho}_B$ such that

$$F(|\Psi\rangle, |\Phi\rangle) = F(\rho_B, \hat{\rho}_B) \geq 1 - \varepsilon.$$

By noting that $F(|\Psi\rangle, |\Phi\rangle)^2 \geq 1 - 2\varepsilon$, from Lemma 9, we have

$$\||\Psi\rangle\langle\Psi| - |\Phi\rangle\langle\Phi|\| \leq \sqrt{8\varepsilon}.$$

Let $\hat{\rho}_{AB} := \mathrm{Tr}_R[|\Phi\rangle\langle\Phi|]$. Then, since the trace distance does not increase by the partial trace, we have

$$\|\rho_{AB} - \hat{\rho}_{AB}\| \leq \sqrt{8\varepsilon}.$$

□

Remark 20 In Lemma 19, if the density operator ρ_{AB} is classical with respect to both systems $\mathcal{H}_A \otimes \mathcal{H}_B$, then we can easily replace $\bar{\varepsilon}$ by ε. Then, $\bar{\varepsilon}$ in Lemma 21, 22 and Corollary 23 can also be replaced by ε.

Lemma 21 Let $\rho_{XB} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_B)$ be a density operator that is classical on $\mathcal{H}_X$. For $\varepsilon \geq 0$, let $\hat{\rho}_B \in \mathcal{B}^\varepsilon(\rho_B)$. Then, there exists a operator $\hat{\rho}_{XB} \in \mathcal{B}^{\bar{\varepsilon}}(\rho_{XB})$ such that $\mathrm{Tr}_X[\hat{\rho}_{XB}] = \hat{\rho}_B$ and $\hat{\rho}_{XB}$ is classical on $\mathcal{H}_X$, where $\bar{\varepsilon} := \sqrt{8\varepsilon}$.

Proof. From Lemma 19, there exists a operator $\rho'_{XB} \in \mathcal{B}^{\bar{\varepsilon}}(\rho_{XB})$ such that $\mathrm{Tr}_X[\rho'_{XB}] = \hat{\rho}_B$. Let $\mathcal{E}_X$ be a projection measurement CP map on $\mathcal{H}_X$, i.e.,

$$\mathcal{E}_X(\rho) := \sum_{x \in \mathcal{X}} |x\rangle\langle x|\rho|x\rangle\langle x|,$$

where $\{|x\rangle\}_{x \in \mathcal{X}}$ is an orthonormal basis of $\mathcal{H}_X$. Let $\hat{\rho}_{XB} := (\mathcal{E}_X \otimes \mathrm{id}_B)(\rho'_{XB})$. Then, since the trace distance does not increase by the CP map, and $(\mathcal{E}_X \otimes \mathrm{id}_B)(\rho_{XB}) = \rho_{XB}$, we have

$$\begin{aligned} &\|\hat{\rho}_{XB} - \rho_{XB}\| \\ &= \|(\mathcal{E}_X \otimes \mathrm{id}_B)(\rho'_{XB}) - (\mathcal{E}_X \otimes \mathrm{id}_B)(\rho_{XB})\| \\ &\leq \|\rho'_{XB} - \rho_{XB}\| \\ &\leq \bar{\varepsilon}. \end{aligned}$$

Furthermore, we have $\mathrm{Tr}_X[\hat{\rho}_{XB}] = \mathrm{Tr}_X[\rho'_{XB}] = \hat{\rho}_B$, and $\hat{\rho}_{XB}$ is classical on $\mathcal{H}_X$. □

The following lemma states that the monotonicity of the min-entropy (Lemma 18) can be extended to the smooth min-entropy by adjusting the smoothness ε.

Lemma 22 Let $\rho_{XBC} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ be a density operator that is classical on $\mathcal{H}_X$. Then, for any $\varepsilon \geq 0$, we have

$$H_{\min}^{\bar{\varepsilon}}(\rho_{XBC}|C) \geq H_{\min}^{\varepsilon}(\rho_{BC}|C),$$

where $\bar{\varepsilon} := \sqrt{8\varepsilon}$.

Proof. We will prove that

$$H_{\min}^{\bar{\varepsilon}}(\rho_{XBC}|\sigma_C) \geq H_{\min}^{\varepsilon}(\rho_{BC}|\sigma_C)$$

holds for any $\sigma_C \in \mathcal{P}(\mathcal{H}_C)$ with $\mathrm{Tr}\sigma_C = 1$. From the definition of the smooth min-entropy, for any $\nu > 0$, there exists $\hat{\rho}_{BC} \in \mathcal{B}^\varepsilon(\rho_{BC})$ such that

$$H_{\min}(\hat{\rho}_{BC}|\sigma_C) \geq H_{\min}^{\varepsilon}(\rho_{BC}|\sigma_C) - \nu. \tag{B2}$$

From Lemma 21, there exists a operator $\hat{\rho}_{XBC} \in \mathcal{B}^{\bar{\varepsilon}}(\rho_{XBC})$ such that $\mathrm{Tr}_X[\hat{\rho}_{XBC}] = \hat{\rho}_{BC}$, and $\hat{\rho}_{XBC}$ is classical on $\mathcal{H}_X$. Then, from Lemma 18, we have

$$H_{\min}(\hat{\rho}_{XBC}|\sigma_C) \geq H_{\min}(\hat{\rho}_{BC}|\sigma_C). \tag{B3}$$

Furthermore, from the definition of smooth min-entropy, we have

$$H_{\min}^{\bar{\varepsilon}}(\rho_{XBC}|\sigma_C) \geq H_{\min}(\hat{\rho}_{XBC}|\sigma_C). \tag{B4}$$

Since $\nu > 0$ is arbitrary, combining Eqs. (B2)–(B4), we have the assertion of the lemma. □

Combining Eq. (B1) of Lemma 17 and Lemma 22, we have the following corollary, which states that the condition decreases the smooth min-entropy by at most the amount of the max-entropy of the condition, and plays an important role to prove security of QKD protocols.

Corollary 23 Let $\rho_{XBC} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ be a density operator that is classical on $\mathcal{H}_X$. Then, for any $\varepsilon \geq 0$, we have

$$H_{\min}^{\bar{\varepsilon}}(\rho_{XBC}|XC) \geq H_{\min}^{\varepsilon}(\rho_{BC}|C) - H_{\max}(\rho_X),$$

where $\bar{\varepsilon} := \sqrt{8\varepsilon}$.

The following lemmas are also used in Section D.

Lemma 24 [14, Theorem 3.2.12] The following inequalities hold:

- Strong sub-additivity:

$$H_{\min}^{\varepsilon}(\rho_{ABC}|BC) \leq H_{\min}^{\varepsilon}(\rho_{AB}|B) \tag{B5}$$

  for $\rho_{ABC} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$.

- Conditioning on classical information:

$$H_{\min}^{\varepsilon}(\rho_{ABZ}|BZ) \geq \min_{z \in \mathcal{Z}} H_{\min}^{\varepsilon}(\rho_{AB}^z|B) \tag{B6}$$

  for $\rho_{ABZ} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_Z)$ normalized and classical on $\mathcal{H}_Z$, and for conditional operators $\rho_{AB}^z \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\rho_B^z \in \mathcal{P}(\mathcal{H}_B)$.

In order to prove that removing the (not necessarily classical) system increases the min-entropy at most the max entropy of the removed system (Lemma 26), we need the following lemma.

Lemma 25 Let $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a density operator, and let $r_A := \mathrm{rank}(\rho_A)$. Then, we have

$$r_A \mathrm{id}_A \otimes \rho_B - \rho_{AB} \geq 0,$$

where id_A is the identity operator on $\mathcal{H}_A$.

Proof. First, we prove the assertion for pure state $\rho_{AB} = |\Psi\rangle\langle\Psi|$. Let

$$|\Psi\rangle = \sum_{i=1}^{r_A} \sqrt{\alpha_i}|\phi_i\rangle \otimes |\psi_i\rangle \tag{B7}$$

be a Schmidt decomposition of $|\Psi\rangle$. Let $\{|\phi_i\rangle\}_{i=1}^{d_A}$ and $\{|\psi_i\rangle\}_{i=1}^{d_B}$ be orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$ that are extensions of vectors in Eq. (B7). For any vector $|\Phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, we can write

$$|\Phi\rangle = \sum_{i=1}^{d_B} \beta_i |\hat{\phi}_i\rangle \otimes |\psi_i\rangle,$$

where $\{|\hat{\phi}_i\rangle\}_{i=1}^{d_B}$ is normalized but not necessarily orthogonal. Then, we have

$$\begin{aligned}\langle\Phi|\rho_{AB}|\Phi\rangle = |\langle\Psi||\Phi\rangle|^2 &= \left|\sum_{i=1}^{r_A} \sqrt{\alpha_i}\beta_i \langle\phi_i||\hat{\phi}_i\rangle\right|^2 \\ &\leq \left|\sum_{i=1}^{r_A} \sqrt{\alpha_i}|\beta_i|\right|^2\end{aligned}$$

and

$$\begin{aligned}\langle\Phi|(r_A \mathrm{id}_A \otimes \rho_B)|\Phi\rangle &= r_A \| \sum_{i=1}^{r_A} \sqrt{\alpha_i}\beta_i |\hat{\phi}_i\rangle \otimes |\psi_i\rangle\|^2 \\ &= r_A \sum_{i=1}^{r_A} \alpha_i |\beta_i|^2.\end{aligned}$$

Using the Cauchy-Schwartz inequality for two vectors $(1, \ldots, 1)$ and $(\sqrt{\alpha_1}|\beta_1|, \ldots, \sqrt{\alpha_{r_A}}|\beta_{r_A}|)$, we have

$$\begin{aligned}\langle\Phi|\rho_{AB}|\Phi\rangle \leq \left|\sum_{i=1}^{r_A} \sqrt{\alpha_i}|\beta_i|\right|^2 &\leq r_A \sum_{i=1}^{r_A} \alpha_i |\beta_i|^2 \\ &= \langle\Phi|(r_A \mathrm{id}_A \otimes \rho_B)|\Phi\rangle.\end{aligned}$$

Thus, the assertion holds for a pure state $\rho_{AB} = |\Psi\rangle\langle\Psi|$. For a mixed state ρ_{AB}, let $\rho_{AB} = \sum_{i=1}^m p_i |\Psi_i\rangle\langle\Psi_i|$ be an eigenvalue decomposition. Let $\rho_B^i = \mathrm{Tr}_A |\Psi_i\rangle\langle\Psi_i|$. Noting that $\mathrm{rank}(\mathrm{Tr}_B |\Psi_i\rangle\langle\Psi_i|) \leq \mathrm{rank}(\mathrm{Tr}_B \rho_{AB}) = r_A$ for all $1 \leq i \leq m$, we have

$$r_A \mathrm{id}_A \otimes \rho_B - \rho_{AB} = \sum_{i=1}^m p_i (r_A \mathrm{id}_A \otimes \rho_B^i - |\Psi_i\rangle\langle\Psi_i|) \geq 0.$$

□

Lemma 26 Let $\rho_{ABC} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ and $\sigma_C \in \mathcal{P}(\mathcal{H}_C)$. Then

$$H_{\min}(\rho_{ABC}|\sigma_C) \geq H_{\min}(\rho_{BC}|\sigma_C) - H_{\max}(\rho_A).$$

Proof. Let λ is such that $H_{\min}(\rho_{BC}|\sigma_C) = -\log\lambda$, i.e., λ is the minimum number satisfying

$$\lambda \mathrm{id}_B \otimes \sigma_C - \rho_{BC} \geq 0.$$

Let $r_A := \mathrm{rank}(\rho_A)$. Then, we want to show that

$$H_{\min}(\rho_{ABC}|\sigma_C) \geq -\log\lambda - \log r_A = -\log r_A\lambda,$$

i.e., $r_A\lambda \mathrm{id}_{AB} \otimes \sigma_C - \rho_{ABC} \geq 0$. From Lemma 25, we have

$$\begin{aligned}&r_A\lambda \mathrm{id}_{AB} \otimes \sigma_C - \rho_{ABC} \\ &\geq r_A\lambda \mathrm{id}_{AB} \otimes \sigma_C - r_A \mathrm{id}_A \otimes \rho_{BC} \\ &= r_A \mathrm{id}_A \otimes (\lambda \mathrm{id}_B \otimes \sigma_C - \rho_{BC}) \geq 0.\end{aligned}$$

□

The following lemma states that Lemma 26 can be extended to the smooth Min-entropy by adjusting the smoothness ε.

Lemma 27 Let $\varepsilon \geq 0$ and $\rho_{ABC} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ be a density operator. Then, we have

$$H_{\min}^{\bar{\varepsilon}}(\rho_{ABC}|C) \geq H_{\min}^{\varepsilon}(\rho_{BC}|C) - \log\dim\mathcal{H}_A,$$

where $\bar{\varepsilon} := \sqrt{8\varepsilon}$.

Proof. We will prove that

$$H_{\min}^{\bar{\varepsilon}}(\rho_{ABC}|\sigma_C) \geq H_{\min}^{\varepsilon}(\rho_{BC}|\sigma_C) - \log\dim\mathcal{H}_A$$

holds for any $\sigma_C \in \mathcal{P}(\mathcal{H}_C)$ with $\mathrm{Tr}\sigma_C = 1$. For any $\nu > 0$, there exists $\hat{\rho}_{BC} \in \mathcal{B}^{\varepsilon}(\rho_{BC})$ such that

$$H_{\min}(\hat{\rho}_{BC}|\sigma_C) \geq H_{\min}^{\varepsilon}(\rho_{BC}|\sigma_C) - \nu. \tag{B8}$$

From Lemma 19, there exists a operator $\hat{\rho}_{ABC} \in \mathcal{B}^{\bar{\varepsilon}}(\rho_{ABC})$ such that $\mathrm{Tr}_A[\hat{\rho}_{ABC}] = \hat{\rho}_{BC}$. Then from Lemma 26, we have

$$H_{\min}(\hat{\rho}_{ABC}|\sigma_C) \geq H_{\min}(\hat{\rho}_{BC}|\sigma_C) - \log\dim\mathcal{H}_A. \tag{B9}$$

Furthermore, from the definition of the smooth-min-entropy, we have

$$H_{\min}^{\bar{\varepsilon}}(\rho_{ABC}|\sigma_C) \geq H_{\min}(\hat{\rho}_{ABC}|\sigma_C). \tag{B10}$$

Since $\nu > 0$ is arbitrary, combining Eqs. (B8)–(B10), we have the assertion of the lemma. □

Lemma 28 For density operators $\rho_{AB}, \overline{\rho}_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ such that $\|\rho_{AB} - \overline{\rho}_{AB}\| \leq \varepsilon'$, we have

$$H_{\min}^{\varepsilon}(\rho_{AB}|B) \leq H_{\min}^{\varepsilon+\varepsilon'}(\overline{\rho}_{AB}|B)$$

Proof. For all $\hat{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})$, by the triangle inequality, we have

$$\|\overline{\rho}_{AB} - \hat{\rho}_{AB}\| \leq \|\rho_{AB} - \hat{\rho}_{AB}\| + \|\overline{\rho}_{AB} - \rho_{AB}\| \leq \varepsilon + \varepsilon'.$$

Thus, we have $\hat{\rho}_{AB} \in \mathcal{B}^{\varepsilon+\varepsilon'}(\overline{\rho}_{AB})$, and

$$H_{\min}^{\varepsilon}(\rho_{AB}|\sigma_B) \leq H_{\min}^{\varepsilon+\varepsilon'}(\overline{\rho}_{AB}|\sigma_B)$$

for all $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$. Then we have the assertion of the lemma. □

2. Privacy amplification

The following definition is used to state the security of the distilled key by the privacy amplification.

Definition 29 [14, Definition 5.2.1] Let $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Then the trace distance from the uniform of ρ_{AB} given B is defined by

$$d(\rho_{AB}|B) := \|\rho_{AB} - \rho_A^{\mathrm{mix}} \otimes \rho_B\|,$$

where $\rho_A^{\mathrm{mix}} := \frac{1}{\dim \mathcal{H}_A}\mathrm{id}_A$ is the fully mixed state on $\mathcal{H}_A$ and $\rho_B := \mathrm{Tr}_A[\rho_{AB}]$.

Definition 30 [40] Let $\mathcal{F}$ be a family of hash functions from $\mathcal{X}$ to $\mathcal{Z}$, and let P_F be the uniform probability distribution on $\mathcal{F}$. The family $\mathcal{F}$ is called two-universal if $\Pr\{f(x) = f(x')\} \leq \frac{1}{|\mathcal{Z}|}$ for any distinct $x, x' \in \mathcal{X}$.

Consider an operator $\rho_{XB} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_B)$ that is classical with respect to an orthonormal basis $\{|x\rangle\}_{x\in\mathcal{X}}$ of $\mathcal{H}_X$, and assume that f is a function from $\mathcal{X}$ to $\mathcal{Z}$. The operator describing the classical function output together with the quantum system $\mathcal{H}_B$ is then given by

$$\rho_{f(X)B} := \sum_{z\in\mathcal{Z}} |z\rangle\langle z| \otimes \rho_B^z \text{ for } \rho_B^z := \sum_{x\in f^{-1}(z)} \rho_B^x, \quad \text{(B11)}$$

where $\{|z\rangle\}_{z\in\mathcal{Z}}$ is an orthonormal basis of $\mathcal{H}_Z$.

Assume now that the function f is randomly chosen from a family $\mathcal{F}$ of function according to the uniform probability distribution P_F. Then the output $f(x)$, the state of the quantum system, and the choice of the function f is described by the operator

$$\rho_{F(X)BF} := \sum_{f\in\mathcal{F}} P_F(f)\rho_{f(X)B} \otimes |f\rangle\langle f| \quad \text{(B12)}$$

on $\mathcal{H}_Z \otimes \mathcal{H}_B \otimes \mathcal{H}_F$, where $\mathcal{H}_F$ is a Hilbert space with orthonormal basis $\{|f\rangle\}_{f\in\mathcal{F}}$. The system $\mathcal{H}_Z$ describes the distilled key, and the system $\mathcal{H}_B$ and $\mathcal{H}_F$ describe the information which an adversary Eve can access. The following lemma states that the length of securely distillable key is given by the conditional smooth min-entropy $H_{\min}^{\varepsilon}(\rho_{XB}|B)$.

Lemma 31 [14, Corollary 5.6.1] Let $\rho_{XB} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_B)$ be a density operator which is classical with respect to an orthonormal basis $\{|x\rangle\}_{x\in\mathcal{X}}$ of $\mathcal{H}_X$. Let $\mathcal{F}$ be a two-universal family of hash functions from $\mathcal{X}$ to $\{0,1\}^{\ell}$, and let $\varepsilon \geq 0$. Then we have

$$d(\rho_{F(X)BF}|BF) \leq 2\varepsilon + 2^{-\frac{1}{2}(H_{\min}^{\varepsilon}(\rho_{XB}|B)-\ell)}$$

for $\rho_{F(X)BF} \in \mathcal{P}(\mathcal{H}_Z \otimes \mathcal{H}_B \otimes \mathcal{H}_F)$ defined by Eq. (B12).

APPENDIX C: SYMMETRIC STATES

In this section, we review the property of symmetric states and the de Finetti style representation theorem [14, 30]. For more detail, refer to [14, Section 4].

Let $\mathcal{H}$ be a Hilbert space and let $\mathcal{S}_n$ be the set of permutations on $\{1, \ldots, n\}$. For any $\pi \in \mathcal{S}_n$, we denote by the same letter π the unitary operation on $\mathcal{H}^{\otimes n}$ which permutes the n subsystems, that is,

$$\pi(|\theta_1\rangle \otimes \cdots \otimes |\theta_n\rangle) := |\theta_{\pi^{-1}(1)}\rangle \otimes \cdots \otimes |\theta_{\pi^{-1}(n)}\rangle,$$

for any $|\theta_1\rangle, \ldots, |\theta_n\rangle \in \mathcal{H}$.

Definition 32 [14, Definition 4.1.1] The symmetric subspace $\mathrm{Sym}(\mathcal{H}^{\otimes n})$ of $\mathcal{H}^{\otimes n}$ is the subspace of $\mathcal{H}^{\otimes n}$ spanned by all vectors which are invariant under permutations of the subsystems, that is,

$$\mathrm{Sym}(\mathcal{H}^{\otimes n}) := \{|\Psi\rangle \in \mathcal{H}^{\otimes n} \mid \pi|\Psi\rangle = |\Psi\rangle,\ \forall \pi \in \mathcal{S}_n\}.$$

Definition 33 [14, Definition 4.1.4] Let $|\theta\rangle \in \mathcal{H}$ be fixed, and let $0 \leq m \leq n$. We denote by $\mathcal{V}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes m})$ the set of vectors $|\Psi\rangle \in \mathcal{H}^{\otimes n}$ which, after some reordering of the subsystems, are of the form $|\theta\rangle^{\otimes m} \otimes |\tilde{\Psi}\rangle$, that is,

$$\begin{aligned}&\mathcal{V}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes m})\\ &:= \{\pi(|\theta\rangle^{\otimes m} \otimes |\tilde{\Psi}\rangle) \mid \pi \in \mathcal{S}_n,\ |\tilde{\Psi}\rangle \in \mathcal{H}^{\otimes n-m}\}.\end{aligned}$$

The symmetric subspace $\mathrm{Sym}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes m})$ of $\mathcal{H}^{\otimes n}$ along $|\theta\rangle^{\otimes m}$ is

$$\mathrm{Sym}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes m}) := \mathrm{Sym}(\mathcal{H}^{\otimes n}) \cap \mathrm{span}\ \mathcal{V}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes m}).$$

If $m \ll n$, then we can consider that a state $|\Psi\rangle \in \mathrm{Sym}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes m})$ is almost the same as the product state $|\theta\rangle^{\otimes n}$.

The following lemma states that a permutation invariant mixed states have a purification in the symmetric space of a extended systems.

Lemma 34 [14, Lemma 4.2.2] Let $\rho_n \in \mathcal{P}(\mathcal{H}^{\otimes n})$ be permutation-invariant. Then, there exists a purification $|\Psi\rangle \in \mathrm{Sym}((\mathcal{H} \otimes \mathcal{H})^{\otimes n})$ of ρ_n.

The following lemma states that a pure state on a symmetric space can be approximated by a convex combination of pure states that are close to a product state.

Lemma 35 [14, Theorem 4.3.2] Let ρ_{n+k} be a pure state density operator on $\mathrm{Sym}(\mathcal{H}^{\otimes n+k})$ and let $0 \le r \le n$. Then, there exists a measure ν on $\mathcal{S}_1(\mathcal{H}) := \{|\theta\rangle \in \mathcal{H} \mid \||\theta\rangle\| = 1\}$ and a pure density operator $\bar{\rho}_n^{|\theta\rangle}$ on $\mathrm{Sym}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes n-r})$ for each $|\theta\rangle \in \mathcal{S}_1(\mathcal{H})$ such that

$$\left\| \mathrm{Tr}_k(\rho_{n+k}) - \int_{\mathcal{S}_1(\mathcal{H})} \bar{\rho}_n^{|\theta\rangle} \nu(|\theta\rangle) \right\| \le 2e^{-\frac{k(r+1)}{2(n+k)} + \frac{1}{2}\dim(\mathcal{H})\ln k},$$

where the base of ln is e.

The following lemma states that the smooth min-entropy of a density operator that is derived from a pure state on $\mathrm{Sym}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes n-m})$ can be approximated from below by the von Neumann entropy of a density operator that is derived from a product state $|\theta\rangle^{\otimes n}$.

Lemma 36 [14, Theorem 4.4.1] Let $0 \le r \le \frac{1}{2}n$, $|\theta\rangle \in \mathcal{H}$, and $|\Psi\rangle \in \mathrm{Sym}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes n-r})$ be normalized, and let $\mathcal{E}$ be a trace-preserving CP map from $\mathcal{H}$ to $\mathcal{H}_X \otimes \mathcal{H}_B$ that is classical on $\mathcal{H}_X$, i.e., $\mathcal{E}(\rho)$ is a $\{cq\}$-state for any $\rho \in \mathcal{P}(\mathcal{H})$. Define $\rho_{X^nB^n} := \mathcal{E}^{\otimes n}(|\Psi\rangle\langle\Psi|)$ and $\sigma_{XB} := \mathcal{E}(|\theta\rangle\langle\theta|)$. Then, for any $\varepsilon > 0$,

$$\frac{1}{n} H_{\min}^{\varepsilon}(\rho_{X^nB^n}|B^n) \ge H(\sigma_{XB}) - H(\sigma_B) - \delta,$$

where $\delta = (\frac{5}{2}H_{\max}(\sigma_X) + 4)\sqrt{\frac{2\log(4/\varepsilon)}{n}} + h(r/n)$.

Lemma 37 [14, Theorem 4.5.2] Let $0 \le r \le \frac{1}{2}n$, $|\theta\rangle \in \mathcal{H}$, and $|\Psi\rangle \in \mathrm{Sym}(\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes n-r})$ be normalized. Let $\mathcal{M} = \{M_z\}_{z\in\mathcal{Z}}$ be a POVM on $\mathcal{H}$, and let P_Z be a probability distribution of the outcomes of the measurement $\mathcal{M}$ applied to $|\theta\rangle\langle\theta|$. Then we have

$$\Pr_{\mathbf{z}}[\|P_{\mathbf{z}} - P_Z\| > \alpha] \le \varepsilon$$

for

$$\alpha := 2\sqrt{\frac{\log(1/\varepsilon)}{n} + h(r/n) + \frac{|\mathcal{Z}|}{n}\log(\frac{n}{2}+1)}$$

where the probability is taken over the outcomes $\mathbf{z} = (z_1, \ldots, z_n)$ of the product measurement $\mathcal{M}^{\otimes n}$ applied to $|\Psi\rangle\langle\Psi|$.

Lemma 37 states that if the product measurement $\mathcal{M}^{\otimes n}$ is applied to $|\Psi\rangle\langle\Psi|$, then the probability such that type $P_{\mathbf{z}}$ of the outcomes deviates from the distribution P_Z is small.

APPENDIX D: PROOF OF THEOREM 2

In this section, we prove Theorem 2. In Section D 1, we first prove the security agaist known adversary. In Section D 2, we analyze the parameter estimation protocol. Then, using results in Sections D 1 and D 2, we prove Theorem 2.

1. Security against known adversary

In this section, we analyze a situation after the parameter estimation of the QKD protocols, i.e., we assume the following situation. Alice and Bob have $2n$-bit binary sequences $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n}$ that is distributed according to a probability distribution $P_{\mathbf{XY}}$, and Eve can access the quantum system $\mathcal{H}_E$ whose state $\rho_E^{\mathbf{x},\mathbf{y}}$ is correlated to $(\mathbf{x}, \mathbf{y})$. This situation can be described by a $\{ccq\}$-state

$$\rho_{\mathbf{XY}E} := \sum_{(\mathbf{x},\mathbf{y})} P_{\mathbf{XY}}(\mathbf{x},\mathbf{y})|\mathbf{x},\mathbf{y}\rangle\langle\mathbf{x},\mathbf{y}| \otimes \rho_E^{\mathbf{x},\mathbf{y}}.$$

In the following, we follow the notations of Section 2 even though the distribution $P_{\mathbf{XY}}$ is not necessarily the product distribution P_{XY}^{2n}.

In order to agree on a secure key pair (S_A, S_B), Alice and Bob perform the procedure as in Section 3. Then, the situation after the IR protocol and the privacy amplification can be described by a $\{ccq\}$-state

$$\rho_{S_AS_BCE} := \sum_{(s_A,s_B)} P_{S_AS_B}(s_A,s_B)|s_A,s_B\rangle\langle s_A,s_B| \otimes \rho_{CE}^{s_A,s_B},$$

where the classical system C describes the exchanged messages $(\mathbf{T}_1, \hat{\mathbf{T}}_2, \hat{\mathbf{W}}_1)$ in the IR protocol and the choice F of the hash function in the PA protocol. As in Section 3, the distilled key pair (S_A, S_B) is said to be ε-secure if

$$\frac{1}{2}\|\rho_{S_AS_BE'} - \rho_{S_AS_B}^{\mathrm{mix}} \otimes \rho_{E'}\| \le \varepsilon, \tag{D1}$$

where $\rho_{S_AS_B}^{\mathrm{mix}} := \sum_{s\in\mathcal{S}} \frac{1}{|\mathcal{S}|}|s,s\rangle\langle s,s|$ is the uniformly distributed key on $\mathcal{S}$. The above security definition for the key distillation protocol can be subdivided into two parts (see also [14, Remark 6.1.3]):

- The distilled key pair (S_A, S_B) is ε_c-correct if
$$\sum_{s_A \ne s_B} P_{S_AS_B}(s_A, s_B) \le \varepsilon_c.$$
- The distilled key S_A is ε_s-secret if $\frac{1}{2}d(\rho_{S_AE'}|E') \le \varepsilon_s$.

In particular, if the distilled key (s_A, s_B) is ε_c-correct and ε_s-secret, then it is $(\varepsilon_c + \varepsilon_s)$-secure.

The following theorem gives the relation between the security and the length of distilled key.

Theorem 38 Assume that Alice and Bob's bit sequence after the IR protocol are identical to $\mathbf{u}$ with probability at least $1-\varepsilon_1$, i.e.,

$$P_{\mathbf{XY}}(\{(\mathbf{x},\mathbf{y}) : \hat{\mathbf{u}} = \tilde{\mathbf{u}} = \mathbf{u}\}) \geq 1-\varepsilon_1. \tag{D2}$$

For a given number $R, R_0 > 0$, assume that the rate of linear codes that are used in the IR protocol satisfy $\frac{m}{n} \leq R$ and $\frac{m_0}{n_0} \leq R_0$ for all $\underline{n}_0 \leq n_0 \leq \overline{n}_0$. Furthermore assume that the length ℓ of the distilled key by the privacy amplification satisfies

$$\begin{aligned}\ell \leq \max[&H_{\min}^{\varepsilon}(\rho_{\mathbf{UW}_1E}|\mathbf{W}_1E) - nR - \overline{n}_0R_0, \\ &H_{\min}^{\varepsilon}(\rho_{\mathbf{UW}_1\mathbf{U}_1E}|\mathbf{W}_1\mathbf{U}_1E) - \overline{n}_0R_0] - \log(1/8\varepsilon)\end{aligned} \tag{D3}$$

where $\rho_{\mathbf{UW}_1E}$ and $\rho_{\mathbf{UW}_1\mathbf{U}_1E}$ are derived from $\rho_{\mathbf{XY}E}$ by using the functions ξ_1 and ξ_2 in the same way as in Section 2. Then the distilled key pair (S_A, S_B) is $(\bar{\varepsilon}+3\varepsilon_1)$-secure, where $\bar{\varepsilon} := \frac{3}{2}\sqrt{8\varepsilon}$.

Proof. First, we will prove that the dummy key $S := f(\mathbf{U})$ is $\bar{\varepsilon}$-secret under the condition that Eve can access $(\mathbf{W}_1, \mathbf{T}_1, \mathbf{T}_2, F, E)$, i.e.,

$$\frac{1}{2}\|\rho_{S\mathbf{W}_1\mathbf{T}_1\mathbf{T}_2FE} - \rho_S^{\mathrm{mix}} \otimes \rho_{\mathbf{W}_1\mathbf{T}_1\mathbf{T}_2FE}\| \leq \bar{\varepsilon}. \tag{D4}$$

The assumption that Alice and Bob's bit sequence are identical to $\mathbf{u}$ with probability $1-\varepsilon_1$ implies that $\hat{\mathbf{w}}_1 = \mathbf{w}_1$ and $\hat{\mathbf{t}}_2 = \mathbf{t}_2$ with probability $1-\varepsilon_1$. Since $(\mathbf{u}, \hat{\mathbf{u}})$, $(\mathbf{w}_1, \hat{\mathbf{w}}_1)$, and $(\mathbf{t}_2, \hat{\mathbf{t}}_2)$ can be computed from $(\mathbf{x}, \mathbf{y})$, by using Lemma 7, we have

$$\|\rho_{\mathbf{XY}\hat{\mathbf{U}}\hat{\mathbf{W}}_1\mathbf{T}_1\hat{\mathbf{T}}_2FE} - \rho_{\mathbf{XYUW}_1\mathbf{T}_1\mathbf{T}_2FE}\| \leq 2\varepsilon_1.$$

Since the trace distance does not increase by CP maps, we have

$$\|\rho_{S_A\hat{\mathbf{W}}_1\mathbf{T}_1\hat{\mathbf{T}}_2FE} - \rho_{S\mathbf{W}_1\mathbf{T}_1\mathbf{T}_2FE}\| \leq 2\varepsilon_1.$$

Thus the statement that the dummy key S is $\bar{\varepsilon}$-secret implies that the actual key S_A is $(\bar{\varepsilon}+2\varepsilon_1)$-secret as follows:

$$\begin{aligned}&\|\rho_{S_A\hat{\mathbf{W}}_1\mathbf{T}_1\hat{\mathbf{T}}_2FE} - \rho_{S_A}^{\mathrm{mix}} \otimes \rho_{\hat{\mathbf{W}}_1\mathbf{T}_1\hat{\mathbf{T}}_2FE}\| \\ &\leq \|\rho_{S_A\hat{\mathbf{W}}_1\mathbf{T}_1\hat{\mathbf{T}}_2FE} - \rho_{S\mathbf{W}_1\mathbf{T}_1\mathbf{T}_2FE}\| \\ &\quad + \|\rho_{S\mathbf{W}_1\mathbf{T}_1\mathbf{T}_2FE} - \rho_S^{\mathrm{mix}} \otimes \rho_{\mathbf{W}_1\mathbf{T}_1\mathbf{T}_2FE}\| \\ &\quad + \|\rho_S^{\mathrm{mix}} \otimes \rho_{\mathbf{W}_1\mathbf{T}_1\mathbf{T}_2FE} - \rho_{S_A}^{\mathrm{mix}} \otimes \rho_{\hat{\mathbf{W}}_1\mathbf{T}_1\hat{\mathbf{T}}_2FE}\|,\end{aligned}$$

where the first term is upper bounded by $2\varepsilon_1$, the second term is upper bounded by $\bar{\varepsilon}$, and the third term is also upper bounded by $2\varepsilon_1$ because $\rho_S^{\mathrm{mix}} = \rho_{S_A}^{\mathrm{mix}}$. The assumption of Eq. (D2) also implies that the distilled key is ε_1-correct. Thus the distilled key pair (S_A, S_B) is $(\bar{\varepsilon}+3\varepsilon_1)$-secure.

In order to prove Eq. (D4), we use Lemma 31, which gives the relation between the security and the length of the distilled key. If the length ℓ of the distilled key by the privacy amplification satisfies

$$\log(1/8\varepsilon) + \ell \leq H_{\min}^{\sqrt{8\varepsilon}}(\rho_{\mathbf{UW}_1\mathbf{T}_1\mathbf{T}_2E}|\mathbf{W}_1\mathbf{T}_1\mathbf{T}_2E), \tag{D5}$$

then the distilled key S is $\bar{\varepsilon}$-secret. By using Corollary 23, we can lower bound the r.h.s. of Eq. (D5) by

$$H_{\min}^{\varepsilon}(\rho_{\mathbf{UW}_1E}|\mathbf{W}_1E) - nR - \overline{n}_0R_0,$$

because the size of messages $\mathbf{T}_1$ and $\mathbf{T}_2$ are upper bounded by nR and $\overline{n}_0R_0$ respectively. Thus we have shown the statement of the theorem for the first argument of the maximum in Eq. (D3).

Since the syndrome $\mathbf{T}_1$ is computed from the sequence $\mathbf{U}_1$, if the distilled key S is $\bar{\varepsilon}$-secret in the case that Eve can access the sequence $\mathbf{U}_1$, then the distilled key S is $\bar{\varepsilon}$-secret in the case that Eve can only access the syndrome $\mathbf{T}_1$ instead of the sequence $\mathbf{U}_1$. Again using Lemma 31, if the length of the distilled key satisfies

$$\log(1/8\varepsilon) + \ell \leq H_{\min}^{\sqrt{8\varepsilon}}(\rho_{\mathbf{UW}_1\mathbf{U}_1\mathbf{T}_2E}|\mathbf{W}_1\mathbf{U}_1\mathbf{T}_2E), \tag{D6}$$

then the distilled key S is $\bar{\varepsilon}$-secret. Again using Corollary 23, we can lower bound the r.h.s. of Eq. (D6) by

$$H_{\min}^{\varepsilon}(\rho_{\mathbf{UW}_1\mathbf{U}_1E}|\mathbf{W}_1\mathbf{U}_1E) - \overline{n}_0R_0.$$

Thus we have shown the statement of the theorem for the second argument of the maximum in Eq. (D3). □

2. Fluctuation of the actual error rate

In this section, we show that the parameter estimation works with high probability (Lemma 39). Then, we show that the information reconciliation protocol works for symmetric errors if the protocol universally works for the i.i.d. errors that are close to the estimated error distributions in the parameter estimation protocol (Lemma 40).

For the output $Q \in \mathcal{Q}$ of the parameter estimation protocol, let

$$\Gamma_\mu(Q) := \{\sigma_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B) \mid \|P_A^{\sigma_{AB}} - Q\| \leq \mu\}$$

be a set of two-qubit density operators that are compatible with the output Q with a fluctuation μ, where $P_A^{\sigma_{AB}}$ denotes the probability distribution of the outcomes when measuring σ_{AB} by the POVM $\mathcal{M}$, i.e., $P_A^{\sigma_{AB}}(a) := \mathrm{Tr}[M_a\sigma_{AB}]$. When $\rho_m = \sigma_{AB}^{\otimes m}$ is a product state for $\sigma_{AB} \notin \Gamma_\mu(Q)$, then by the law of large numbers, the probability such that the parameter estimation protocol outputs the type Q is negligible. The following lemma generalize this statement to permutation-invariant states.

Lemma 39 [14, Lemma 6.2.2] Let $0 \leq r \leq \frac{1}{2}m$. Moreover, let $|\theta\rangle \in \mathcal{H}_{ABE} := \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$, and let $\rho_{A^mB^mE^m}^{|\theta\rangle}$ be a density operator on $\mathrm{Sym}(\mathcal{H}_{ABE}^{\otimes m}, |\theta\rangle^{\otimes m-r})$. For any $\varepsilon_{\mathsf{P}} > 0$, if $\mathrm{Tr}_E|\theta\rangle\langle\theta| \notin \Gamma_\mu(Q)$ for

$$\mu = 2\sqrt{\frac{\log(1/\varepsilon_{\mathsf{P}})}{m} + h(r/m) + \frac{|\mathcal{W}|}{m}\log(\frac{m}{2}+1)}, \tag{D7}$$

then the probability such that the parameter estimation protocol outputs Q is at most ε_{P}, i.e., $\mathcal{E}_Q(\rho^{|\theta\rangle}_{A^mB^m}) \leq \varepsilon_{\mathsf{P}}$.

For the POVM $\mathcal{M}_{XY}$, which is used for obtaining the raw keys in the QKD protocol, let $P^{\sigma_{AB}}_{XY}$ be the probability distribution of the outcomes when measuring σ_{AB} by the POVM $\mathcal{M}_{XY}$, i.e., $P^{\sigma_{AB}}_{XY}(x,y) := \mathrm{Tr}[M_{xy}\sigma_{AB}]$. For

$$\bar{\mu} = 2\sqrt{\frac{\log(1/\varepsilon_2)}{2n} + h(r/2n) + \frac{\log(n+1)}{n}}, \tag{D8}$$

let

$$\mathcal{Q}_{\bar{\mu}}(Q) := \{P \in \mathcal{P}_{2n}(\mathbb{F}_2^2) \mid \min_{\sigma_{AB}\in\Gamma_\mu(Q)} \|P^{\sigma_{AB}}_{XY} - P\| \leq \bar{\mu}\}$$

be a subset of all types on $\mathbb{F}_2^2$. Note that if we measure a product state $\sigma_{AB}^{\otimes 2n}$ of $\sigma_{AB} \in \Gamma_\mu(Q)$ by the product POVM $\mathcal{M}_{XY}^{\otimes 2n}$, then the joint type $P_{\mathbf{xy}}$ of the outcomes is contained in the set $\mathcal{Q}_{\bar{\mu}}(Q)$ with high probability.

Lemma 40 Let $\rho^{|\theta\rangle}_{A^{2n}B^{2n}E^{2n}}$ be a density operator on $\mathrm{Sym}(\mathcal{H}_{ABE}^{\otimes 2n}, |\theta\rangle^{\otimes 2n-r})$. Let $P^{|\theta\rangle}_{\mathbf{XY}} \in \mathcal{P}(\mathbb{F}_2^{2n}\times\mathbb{F}_2^{2n})$ be a probability distribution of the outcomes when measuring $\rho^{|\theta\rangle}_{A^{2n}B^{2n}}$ by the POVM $\mathcal{M}_{XY}^{\otimes 2n}$. Assume that Alice and Bob's bit sequence after the IR protocol are identical to $\mathbf{u}$ with probability at least $1-\varepsilon_1$ for any probability distribution $P \in \mathcal{Q}_{\bar{\mu}}(Q)$, i.e.,

$$P^{2n}(\{(\mathbf{x},\mathbf{y}) : \hat{\mathbf{u}} \neq \mathbf{u} \text{ or } \tilde{\mathbf{u}} \neq \mathbf{u}\}) \leq \varepsilon_1. \tag{D9}$$

If $\mathrm{Tr}_E|\theta\rangle\langle\theta| \in \Gamma_\mu(Q)$, then we have

$$P^{|\theta\rangle}_{\mathbf{XY}}(\{(\mathbf{x},\mathbf{y}) : \hat{\mathbf{u}} \neq \mathbf{u} \text{ or } \tilde{\mathbf{u}} \neq \mathbf{u}\}) \leq L\varepsilon_1 + \varepsilon_2, \tag{D10}$$

where $L := (2n+1)^3$, and ε_2 is given in Eq. (D8).

Proof. For each type $P \in \mathcal{P}_{2n}(\mathbb{F}_2\times\mathbb{F})$, let

$$\gamma_P := \frac{|\{(\mathbf{x},\mathbf{y}) : \hat{\mathbf{u}} \neq \mathbf{u} \text{ or } \tilde{\mathbf{u}} \neq \mathbf{u}\} \cap \mathcal{T}_P^{2n}|}{|\mathcal{T}_P^{2n}|}$$

be the ratio of pairs of sequences in $\mathcal{T}_P^{2n}$ such that Alice or Bob's sequences after the IR protocol are not identical to $\mathbf{u}$. Since the distribution $P^{|\theta\rangle}_{\mathbf{XY}}$ is permutation invariant, we can rewrite the l.h.s. of Eq. (D10) as

$$\sum_{P\in\mathcal{Q}_{\bar{\mu}}(Q)} \gamma_P P^{|\theta\rangle}_{\mathbf{XY}}(\mathcal{T}_P^{2n}) + \sum_{P\notin\mathcal{Q}_{\bar{\mu}}(Q)} \gamma_P P^{|\theta\rangle}_{\mathbf{XY}}(\mathcal{T}_P^{2n}). \tag{D11}$$

Since $\mathrm{Tr}_E|\theta\rangle\langle\theta| \in \Gamma_\mu(Q)$, by using Lemma 37, the second term of Eq. (D11) is upper bounded by ε_2.

On the other hand, by using Eq. (A3), we have

$$\varepsilon_1 \geq \gamma_P P^{2n}(\mathcal{T}_P^{2n}) \geq \frac{\gamma_P}{(2n+1)^3}$$

for any $P \in \mathcal{Q}_{\bar{\mu}}(Q)$. Thus, the first term of Eq. (D11) is upper bounded by $(2n+1)^3\varepsilon_1$. □

3. Security poof

In order to save space, we abbreviate $2n+m$ by K. In this section, if there are two operators $\rho \in \mathcal{P}(\mathcal{H})$ and $\tilde{\rho} \in \mathcal{P}(\mathcal{H})$, then the former represents the normalized density operator of the latter, i.e., $\rho = \frac{1}{\mathrm{Tr}\tilde{\rho}}\tilde{\rho}$.

a. Parameter estimation

We first analyze the situation after the parameter estimation protocol is executed. More specifically, by using Lemmas 35 and 39, we will show Eq. (D13), which states that the density operator $\rho^Q_{A^{2n}B^{2n}E^{2n}}$ after the parameter estimation protocol can be approximated by a convex combination of almost product states.

Since the tripartite state $\rho_{A^NB^NE^N}$ lies on the symmetric subspace of $\mathcal{H}_{ABE}^{\otimes N} := (\mathcal{H}_A\otimes\mathcal{H}_B\otimes\mathcal{H})^{\otimes N}$, by using Lemma 35, the density operator $\rho_{A^KB^KE^K}$ is approximated by a convex combination of almost product states, i.e.,

$$\|\rho_{A^KB^KE^K} - \int_{\mathcal{S}_1} \rho^{|\theta\rangle}_{A^KB^KE^K}\nu(|\theta\rangle)\| \leq \kappa,$$

where the integral runs over the set $\mathcal{S}_1 := \mathcal{S}_1(\mathcal{H}_{ABE})$ of normalized vectors on $\mathcal{H}_{ABE}$, where

$$\rho^{|\theta\rangle}_{A^KB^KE^K} \in \mathcal{P}(\mathrm{Sym}(\mathcal{H}_{ABE}^{\otimes K}, |\theta\rangle^{\otimes K-r}))$$

for any $|\theta\rangle \in \mathcal{S}_1$, and where

$$r := \frac{2N}{k}\{\ln(2/\kappa) + \dim(\mathcal{H}_A\otimes\mathcal{H}_B)\cdot\ln k\}.$$

Since the trace distance does not increase by applying a CP map, we have

$$\|\tilde{\rho}^Q_{A^{2n}B^{2n}E^{2n}} - \int_{\mathcal{S}_1} \tilde{\rho}^{Q,|\theta\rangle}_{A^{2n}B^{2n}E^{2n}}\nu(|\theta\rangle)\| \leq \kappa, \tag{D12}$$

where

$$\tilde{\rho}^{Q,|\theta\rangle}_{A^{2n}B^{2n}E^{2n}} := (\mathrm{id}_{A^{2n}B^{2n}}\otimes\mathcal{E}_Q\otimes\mathrm{id}_{E^{2n}})(\rho^{|\theta\rangle}_{A^KB^KE^{2n}}).$$

Let

$$\mathcal{V}_\mu := \{|\theta\rangle \in \mathcal{S}_1 \mid \mathrm{Tr}_E|\theta\rangle\langle\theta| \in \Gamma_\mu\}$$

be the subset of $\mathcal{S}_1$ that is compatible with the output Q of the parameter estimation protocol with the fluctuation μ. From Lemma 39, if $|\theta\rangle \notin \Gamma_\mu(Q)$, then the probability such that the parameter estimation protocol outputs Q is at most ε_{P}, i.e., $\|\tilde{\rho}^{Q,|\theta\rangle}_{A^{2n}B^{2n}E^{2n}}\| \leq \varepsilon_{\mathsf{P}}$. Thus, we can restrict the integral in Eq. (D12) to the set $\mathcal{V}_\mu$ as

$$\begin{aligned}
&\|\tilde{\rho}^Q_{A^{2n}B^{2n}E^{2n}} - \tilde{\rho}^{Q,\mathcal{V}_\mu}_{A^{2n}B^{2n}E^{2n}}\| \\
&\leq \|\tilde{\rho}^Q_{A^{2n}B^{2n}E^{2n}} - \int_{\mathcal{S}_1} \tilde{\rho}^{Q,|\theta\rangle}_{A^{2n}B^{2n}E^{2n}}\nu(|\theta\rangle)\| \\
&\quad + \|\int_{\mathcal{V}_\mu^c} \tilde{\rho}^{Q,|\theta\rangle}_{A^{2n}B^{2n}E^{2n}}\nu(|\theta\rangle)\| \leq \kappa + \varepsilon_{\mathsf{P}},
\end{aligned}$$

where we set

$$\tilde{\rho}^{Q,\mathcal{V}_\mu}_{A^{2n}B^{2n}E^{2n}} := \int_{\mathcal{V}_\mu} \tilde{\rho}^{Q,|\theta\rangle}_{A^{2n}B^{2n}E^{2n}} \nu(|\theta\rangle),$$

and $\mathcal{V}_\mu^{\rm c}$ is the complement of $\mathcal{V}_\mu$ in $\mathcal{S}_1$. By using the following Lemma 41, the normalized version of the operators satisfy

$$\|\rho^{Q}_{A^{2n}B^{2n}E^{2n}} - \rho^{Q,\mathcal{V}_\mu}_{A^{2n}B^{2n}E^{2n}}\| \le 2\tilde{\tau}, \tag{D13}$$

where $\tilde{\tau} := \frac{\kappa+\varepsilon_{\mathsf{P}}}{P_{\mathsf{PE}}(Q)}$.

Lemma 41 Let $\tilde{\rho}, \tilde{\sigma} \in \mathcal{P}(\mathcal{H})$ be (not necessarily normalized) operators. Assume that $\|\tilde{\rho} - \tilde{\sigma}\| \le \varepsilon$ for $\varepsilon \ge 0$. Let $\rho := \frac{1}{{\rm Tr}\tilde{\rho}}\tilde{\rho}$ and $\sigma := \frac{1}{{\rm Tr}\tilde{\sigma}}\sigma$ be the normalized operators. Then, we have $\|\rho - \sigma\| \le 2\tilde{\varepsilon}$ for $\tilde{\varepsilon} := \frac{\varepsilon}{{\rm Tr}\tilde{\rho}}$.

Proof. From the assumption, we have $\|\rho - \hat{\sigma}\| \le \tilde{\varepsilon}$, where $\hat{\sigma} := \frac{1}{{\rm Tr}\tilde{\rho}}\sigma$. By using the triangle inequality, we have

$$1 - \tilde{\varepsilon} \le \|\rho\| - \|\rho - \hat{\sigma}\| \le \|\hat{\sigma}\| \le \|\rho\| + \|\hat{\sigma} - \rho\| \le 1 + \tilde{\varepsilon}.$$

Thus, we have

$$\|\sigma - \hat{\sigma}\| = |1 - \|\hat{\sigma}\|| \le \tilde{\varepsilon}.$$

Using once again the triangle inequality, we have

$$\|\rho - \sigma\| \le \|\rho - \hat{\sigma}\| + \|\hat{\sigma} - \sigma\| \le 2\tilde{\varepsilon}.$$

□

b. Information reconciliation

According to Section 2, the IR protocol universally works with a negligible error probability for i.i.d. errors, if we set the parameters $R(Q) = H(P_{W_1}) + \delta$, $R_0(Q) = H(P_{W_2|W_1=0}) + \delta$, $\frac{\overline{n}_0}{n} = P_{W_1}(0) + \delta$, and $\frac{n_0}{n} = P_{W_1}(0) + \delta$. In this section, by using Lemma 40, we show that the IR protocol also works with a negligible error probability in the QKD protocol, i.e.,

$$P^{Q}_{\mathbf{XY}}(\{(\mathbf{x},\mathbf{y}) : \hat{\mathbf{u}} \neq \mathbf{u} \text{ or } \tilde{\mathbf{u}} \neq \mathbf{u}\}) \le \varepsilon_1 + \varepsilon_2 + 2\tilde{\tau}, \tag{D14}$$

where $P^{Q}_{\mathbf{XY}}$ is the probability distribution of the outcomes when measuring $\rho^{Q}_{A^{2n}B^{2n}}$ by $\mathcal{M}^{\otimes 2n}_{XY}$. Note that ε_1 is the error probability of the IR protocol for i.i.d. errors, which exponentially goes to 0 as $n \to \infty$ if we use appropriate linear codes [26, Corollary 2]. As we will see later, ε_2 also exponentially goes to 0 as $n \to \infty$.

By using the fact that the trace distance does not increase by the CP map (measurement by $\mathcal{M}^{\otimes 2n}_{XY}$), the l.h.s. of Eq. (D14) is upper bounded by

$$P^{Q,\mathcal{V}_\mu}_{\mathbf{XY}}(\{(\mathbf{x},\mathbf{y}) : \hat{\mathbf{u}} \neq \mathbf{u} \text{ or } \tilde{\mathbf{u}} \neq \mathbf{u}\}) + 2\tilde{\tau},$$

where $P^{Q,\mathcal{V}_\mu}_{\mathbf{XY}}$ is the probability distribution of the outcomes when measuring $\rho^{Q,\mathcal{V}_\mu}_{A^{2n}B^{2n}}$ by $\mathcal{M}^{\otimes 2n}_{XY}$. Since $\rho^{Q,\mathcal{V}_\mu}_{A^{2n}B^{2n}E^{2n}}$ is a convex combination of density operators $\rho^{Q,|\theta\rangle}_{A^{2n}B^{2n}E^{2n}}$ on ${\rm Sym}(\mathcal{H}^{\otimes 2n}_{ABE}, |\theta\rangle^{\otimes 2n-r})$ such that ${\rm Tr}_E[|\theta\rangle\langle\theta|] \in \Gamma_\mu(Q)$, by using Lemma 40, we have Eq. (D14).

c. Privacy amplification

In this section, we analyze the PA protocol. By applying Theorem 38, if the length $\ell(Q)$ of the distilled key satisfies

$$\begin{aligned}\ell(Q) \le & \\ &\max[H^{\tilde{\varepsilon}}_{\min}(\rho^{Q}_{\mathbf{UW}_1E^N}|\mathbf{W}_1E^N) - nR(Q) - \overline{n}_0R_0(Q), \\ &\quad H^{\tilde{\varepsilon}}_{\min}(\rho_{\mathbf{UW}_1\mathbf{U}_1E^N}|\mathbf{W}_1\mathbf{U}_1E^N) - \overline{n}_0(Q)R_0(Q)] \\ &\quad - \log(1/8\tilde{\varepsilon}),\end{aligned} \tag{D15}$$

then the distilled key is $(3\sqrt{2\tilde{\varepsilon}} + 3\varepsilon_1 + 3\varepsilon_2 + 6\tilde{\tau})$-secure, where $\rho^{Q}_{\mathbf{UW}_1E^N}$ and $\rho_{\mathbf{UW}_1\mathbf{U}_1E^N}$ are derived from $\rho^{Q}_{\mathbf{XY}E^N}$ by using functions ξ_1 and ξ_2 in the same way as in Section 2. Let $\tilde{\varepsilon} := \sqrt{24\tilde{\tau}}$. Multiplying the probability $P_{\mathsf{PE}}(Q)$, the quantities $P_{\mathsf{PE}}(Q)3\sqrt{2\tilde{\varepsilon}} \le 6(6(\kappa+\varepsilon_{\mathsf{P}}))^{1/4}$ and $P_{\mathsf{PE}}(Q)6\tilde{\tau} = 6(\kappa+\varepsilon_{\mathsf{P}})$ goes to 0 as $\kappa, \varepsilon_{\mathsf{P}} \to 0$. Thus, the security of the distilled key, i.e., the l.h.s. of Eq. (2) goes to 0 as $\kappa, \varepsilon_{\mathsf{P}}, \varepsilon_1, \varepsilon_2 \to 0$.

d. Evaluation of key rate

One more thing we have left is to replace the r.h.s. of Eq. (D15) by smaller but more concise equation. Noting that $\kappa + \varepsilon_{\mathsf{P}} \le \tilde{\varepsilon}$, we can replace the last term $\log(1/8\tilde{\varepsilon})$ by $\log(1/8(\kappa+\varepsilon_{\mathsf{P}}))$.

Let $\rho^{Q,|\theta\rangle}_{\mathbf{XY}E^{2n}} := (\mathcal{E}^{\otimes 2n}_{XY} \otimes {\rm id}_{E^{2n}})(\rho^{Q,|\theta\rangle}_{A^{2n}B^{2n}E^{2n}})$, and let $\rho^{Q,|\theta\rangle}_{\mathbf{UW}_1E^{2n}}$ be the density operator derived from $\rho^{Q,|\theta\rangle}_{\mathbf{XY}E^{2n}}$ in the same way as in Section 2. Since $\rho^{Q,|\theta\rangle}_{A^{2n}B^{2n}E^{2n}}$ lies on ${\rm Sym}(\mathcal{H}^{\otimes n}_{A^2B^2E^2}, |\theta^2\rangle^{\otimes n-r})$ for $|\theta^2\rangle := |\theta\rangle^{\otimes 2}$, we can use Lemma 36 to obtain

$$\begin{aligned}&\frac{1}{n}H^{(\kappa+\varepsilon_{\mathsf{P}})}_{\min}(\rho^{Q,|\theta\rangle}_{\mathbf{UW}_1E^{2n}}|\mathbf{W}_1E^{2n}) \\ &\qquad \ge H_\sigma(U_1U_2|W_1E_1E_2) - \delta',\end{aligned} \tag{D16}$$

where

$$\delta' := 9\sqrt{\frac{2\log(4/(\kappa+\varepsilon_{\mathsf{P}}))}{n} + h(r/n)},$$

and where $\sigma_{U_1U_2W_1E_1E_2}$ is derived from $\sigma_{X_1X_2Y_1Y_2E_1E_2} := (\mathcal{E}^{\otimes 2}_{XY} \otimes {\rm id}^{\otimes 2}_E)(|\theta\rangle\langle\theta|^{\otimes 2})$ in the same way as in Section 2.

Let $\rho^{Q,\mathcal{V}_\mu}_{\mathbf{UW}_1E^{2n}}$ be a density operator derived from $\rho^{Q,\mathcal{V}_\mu}_{\mathbf{XY}E^{2n}} := (\mathcal{E}^{\otimes 2}_{XY} \otimes {\rm id}_{E^{2n}})(\rho^{Q,\mathcal{V}_\mu}_{A^{2n}B^{2n}E^{2n}})$ in the same way

as in Section 2. Since $\rho^{Q,\mathcal{V}_\mu}_{\mathbf{U}\mathbf{W}_1E^{2n}}$ is a convex combination of density operators $\rho^{Q,|\theta\rangle}_{\mathbf{U}\mathbf{W}_1E^{2n}}$, by using Eqs. (B5) and (B6) in Lemma 24, we have

$$H_{\min}^{(\kappa+\varepsilon_{\mathsf{P}})}(\rho^{Q,\mathcal{V}_\mu}_{\mathbf{U}\mathbf{W}_1E^{2n}}|\mathbf{W}_1E^{2n}) \geq \min_{|\theta\rangle\in\mathcal{V}_\mu} H_{\min}^{(\kappa+\varepsilon_{\mathsf{P}})}(\rho^{Q,|\theta\rangle}_{\mathbf{U}\mathbf{W}_1E^{2n}}|\mathbf{W}_1E^{2n}). \quad \text{(D17)}$$

Since the trace distance does not increase by a CP map, we have

$$\|\rho^{Q}_{\mathbf{U}\mathbf{W}_1E^{2n}} - \rho^{Q,\mathcal{V}_\mu}_{\mathbf{U}\mathbf{W}_1E^{2n}}\| \leq 2\tilde{\tau}. \quad \text{(D18)}$$

By using (a) Lemmas 17 and 27, (b) Eq. (D18) and Lemma 28, (c) $\kappa+\varepsilon_{\mathsf{P}} \leq \tilde{\tau}$, (d) Eqs. (D16) and (D17), we have

$$\begin{aligned}
\frac{1}{n}H_{\min}^{\sqrt{24\tilde{\tau}}}(\rho^{Q}_{\mathbf{U}\mathbf{W}_1E^{N}}|\mathbf{W}_1E^{N}) &\overset{(a)}{\geq} \frac{1}{n}H_{\min}^{3\tilde{\tau}}(\rho^{Q}_{\mathbf{U}\mathbf{W}_1E^{2n}}|\mathbf{W}_1E^{2n}) - \frac{2(m+k)}{n}\log\dim\mathcal{H}_E \\
&\overset{(b)}{\geq} \frac{1}{n}H_{\min}^{\tilde{\tau}}(\rho^{Q,\mathcal{V}_\mu}_{\mathbf{U}\mathbf{W}_1E^{2n}}|\mathbf{W}_1E^{2n}) - \frac{2(m+k)}{n}\log\dim\mathcal{H}_E \\
&\overset{(c)}{\geq} \frac{1}{n}H_{\min}^{(\kappa+\varepsilon_{\mathsf{P}})}(\rho^{Q,\mathcal{V}_\mu}_{\mathbf{U}\mathbf{W}_1E^{2n}}|\mathbf{W}_1E^{2n}) - \frac{2(m+k)}{n}\log\dim\mathcal{H}_E \\
&\overset{(d)}{\geq} \min_{|\theta\rangle\in\mathcal{V}_\mu} H_\sigma(U_1U_2|W_1E_1E_2) - \delta' - \frac{2(m+k)}{n}\log\dim\mathcal{H}_E.
\end{aligned}$$

In a similar manner, we have

$$\frac{1}{n}H_{\min}^{\sqrt{24\tilde{\tau}}}(\rho^{Q}_{\mathbf{U}\mathbf{W}_1\mathbf{U}_1E^{N}}|\mathbf{W}_1\mathbf{U}_1E^{N}) \geq \min_{|\theta\rangle\in\mathcal{V}_\mu} H_\sigma(U_2|W_1U_1E_1E_2) - \delta' - \frac{2(m+k)}{n}\log\dim\mathcal{H}_E.$$

Finally, setting $k := \alpha_1 n$, $m := \alpha_2 n$, $\kappa := e^{-\alpha_3 k}$, $\varepsilon_{\mathsf{P}} := 2^{-\alpha_4 m}$, $\varepsilon_2 := 2^{-\alpha_5 n}$, and taking $n \to \infty$ and $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \to 0$, we have the assertion of theorem.

APPENDIX E: PROOF OF THEOREM 3

This section presents a proof of Theorem 3 in the main text.

Let

$$\begin{aligned}
|\psi_{ABE}\rangle &:= \sum_{\mathsf{x},\mathsf{z}\in\mathbb{F}_2} \sqrt{P_{\mathsf{X}\mathsf{Z}}(\mathsf{x},\mathsf{z})}|\psi(\mathsf{x},\mathsf{z})\rangle|\mathsf{x},\mathsf{z}\rangle \\
&= \sum_{x,\mathsf{x}\in\mathbb{F}_2} \sqrt{P_{\mathsf{X}}(\mathsf{x})}|x, x+\mathsf{x}\rangle|\phi(x,\mathsf{x})\rangle
\end{aligned}$$

be a purification of $\sigma_{AB} = \sum_{\mathsf{x},\mathsf{z}\in\mathbb{F}_2}|\psi(\mathsf{x},\mathsf{z})\rangle\langle\psi(\mathsf{x},\mathsf{z})|$, where we set

$$|\phi(x,\mathsf{x})\rangle := \frac{1}{\sqrt{P_{\mathsf{X}}(\mathsf{x})}}\sum_{\mathsf{z}\in\mathbb{F}_2}(-1)^{x\mathsf{z}}\sqrt{P_{\mathsf{X}\mathsf{Z}}(\mathsf{x},\mathsf{z})}|\mathsf{x},\mathsf{z}\rangle,$$

and where $P_{\mathsf{X}}(\mathsf{x}) = \sum_{\mathsf{z}\in\mathbb{F}_2}P_{\mathsf{X}\mathsf{Z}}(\mathsf{x},\mathsf{z})$ is a marginal distribution. Then, let

$$\begin{aligned}
&\sigma_{X_1X_2Y_1Y_2E_1E_2} \\
&:= (\mathcal{E}_{XY}^{\otimes 2}\otimes \mathrm{id}_E^{\otimes 2})(|\psi_{ABE}\rangle\langle\psi_{ABE}|^{\otimes 2}) \\
&= \sum_{\vec{x},\vec{\mathsf{x}}\in\mathbb{F}_2^2}\frac{1}{4}P_{\mathsf{X}}^2(\vec{\mathsf{x}})|\vec{x},\vec{x}+\vec{\mathsf{x}}\rangle\langle\vec{x},\vec{x}+\vec{\mathsf{x}}|\otimes\sigma_{E_1E_2}^{\vec{x},\vec{\mathsf{x}}},
\end{aligned}$$

where

$$\sigma_{E_1E_2}^{\vec{x},\vec{\mathsf{x}}} := |\phi(x_1,\mathsf{x}_1)\rangle\langle\phi(x_1,\mathsf{x}_1)|\otimes|\phi(x_2,\mathsf{x}_2)\rangle\langle\phi(x_2,\mathsf{x}_2)|$$

for $\vec{x} = (x_1, x_2)$ and $\vec{\mathsf{x}} = (\mathsf{x}_1, \mathsf{x}_2)$.

Noting that

$$P_{X_1X_2Y_1Y_2}(\vec{x},\vec{x}+\vec{\mathsf{x}}) = \frac{1}{4}P_{\mathsf{X}}^2(\vec{\mathsf{x}}),$$

we have

$$\begin{aligned}
P_{U_1}(u_1) &= \frac{1}{2} \\
P_{W_1}(w_1) &= \sum_{\substack{\vec{\mathsf{x}}\in\mathbb{F}_2^2 \\ \mathsf{x}_1+\mathsf{x}_2=w_1}} P_{\mathsf{X}}^2(\vec{\mathsf{x}}) \\
P_{U_2|W_1=0}(u_2) &= \frac{1}{2} \\
P_{U_2|W_1=1}(u_2) &= 1 \\
P_{W_2|W_1=0}(w_2) &= \frac{P_{\mathsf{X}}^2(w_2,w_2)}{P_{W_1}(w_1)} \\
P_{W_2|W_1=1}(0) &= 1.
\end{aligned}$$

Using these formulas, we can write

$$\begin{aligned}
\sigma_{U_1U_2W_1E_1E_2} = \sum_{\vec{u}\in\mathbb{F}_2^2}\sum_{w_1\in\mathbb{F}_2} & P_{U_1}(u_1)P_{W_1}(w_1) \\
& P_{U_2|W_1=w_1}(u_2)|\vec{u},w_1\rangle\langle\vec{u},w_1|\otimes\bar{\sigma}_{E_1E_2}^{\vec{u},w_1}
\end{aligned}$$

for $\vec{u} = (u_1, u_2)$, where

$$\bar{\sigma}^{\vec{u},w_1}_{E_1E_2} := \sum_{w_2 \in \mathbb{F}_2} P_{W_2|W_1=0}(w_2) \sigma^{\vec{u}G,(w_1,w_2)G}_{E_1E_2}$$

for $w_1 = 0$ and a matrix $G = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, and

$$\bar{\sigma}^{\vec{u},w_1}_{E_1E_2} := \sum_{a,b \in \mathbb{F}_2} \frac{1}{4} \sigma^{(u_1,a)G,(w_1,b)G}_{E_1E_2}$$

for $w_1 = 1$.

Since supports of rank 1 matrices $\{\sigma^{\vec{x},\vec{x}}_{E_1E_2}\}_{\vec{x} \in \mathbb{F}_2^2}$ are orthogonal to each other, $\sigma^{\vec{u},w_1}_{E_1E_2}$ for $w_1 = 0$ is already eigen value decomposed. Applying Lemma 42 for $\mathsf{J} = \{00, 10\}$ and $C = C^\perp = \{00, 11\}$, we can eigen value decompose $\sigma^{\vec{u},w_1}_{E_1E_2}$ for $w_1 = 1$ as

$$\sigma^{\vec{u},w_1}_{E_1E_2} = \sum_{b \in \mathbb{F}_2} \frac{1}{2} \sum_{\vec{\mathsf{j}} \in \mathsf{J}} P_{\mathsf{J}|\bar{\mathsf{X}}=\bar{x}}(\vec{\mathsf{j}}) |\vartheta((u_1,0),\mathsf{x},\vec{\mathsf{j}})\rangle\langle\vartheta((u_1,0),\mathsf{x},\vec{\mathsf{j}})|,$$

where we follow the notations in Lemma 42 for $m = 2$.

Thus, we have

$$\begin{aligned} & H(\sigma_{U_1U_2W_1E_1E_2}) \\ &= H(P_{U_1}) + H(P_{W_1}) + \sum_{w_1 \in \mathbb{F}_2} P_{W_1}(w_1) \{H(P_{U_2|W_1=w_1}) \\ &\quad + \sum_{\vec{u} \in \mathbb{F}_2^2} P_{U_1}(u_1) P_{U_2|W_1=w_1}(u_2) H(\sigma^{\vec{u},w_1}_{E_1E_2})\} \\ &= 1 + H(P_{\bar{\mathsf{X}}}) + P_{\bar{\mathsf{X}}}(0)\{1 + H(P_{\vec{\mathsf{X}}\mathsf{J}|\bar{\mathsf{X}}=0})\} \\ &\quad + P_{\bar{\mathsf{X}}}(1) H(P_{\vec{\mathsf{X}}\mathsf{J}|\bar{\mathsf{X}}=1}). \end{aligned} \tag{E1}$$

Taking the partial trace of $\sigma_{U_1U_2W_1E_1E_2}$ over systems U_1, U_2, we have

$$\begin{aligned} \sigma_{W_1E_1E_2} &= \sum_{w_1 \in \mathbb{F}_2} P_{W_1}(w_1) |w_1\rangle\langle w_1| \\ &\quad \otimes \left(\sum_{\vec{u} \in \mathbb{F}_2^2} P_{U_1} P_{U_2|W_1=w_1}(u_2) \bar{\sigma}^{\vec{u},w_1}_{E_1E_2} \right). \end{aligned}$$

Thus, we have

$$\begin{aligned} H(\sigma_{W_1E_1E_2}) &= H(P_{W_1}) + \sum_{w_1 \in \mathbb{F}_2} P_{W_1}(w_1) \\ &\quad H\left(\sum_{\vec{u} \in \mathbb{F}_2^2} P_{U_1} P_{U_2|W_1=w_1}(u_2) \bar{\sigma}^{\vec{u},w_1}_{E_1E_2} \right) \\ &= H(P_{\bar{\mathsf{X}}}) + \sum_{\bar{x} \in \mathbb{F}_2} P_{\bar{\mathsf{X}}}(0) H(P_{\vec{\mathsf{X}}\vec{\mathsf{Z}}|\bar{\mathsf{X}}=\bar{x}}). \end{aligned} \tag{E2}$$

Combining Eqs. (E1) and (E2), we have

$$\begin{aligned} & H_\sigma(U_1U_2|W_1E_1E_2) - H(P_{W_1}) P_{W_1}(0) H(P_{W_2|W_1=0}) \\ &= 2 - H(P_{\vec{\mathsf{X}}\vec{\mathsf{Z}}}) + P_{\bar{\mathsf{X}}}(1)\{H(P_{\vec{\mathsf{X}}\mathsf{J}|\bar{\mathsf{X}}=1}) - 1\} \\ &= 2 - 2H(P_{\mathsf{XZ}}) + P_{\bar{\mathsf{X}}}(1) h\left(\frac{p_{00}p_{10} + p_{01}p_{11}}{(p_{00}+p_{01})(p_{10}+p_{11})} \right). \end{aligned}$$

On the other hand, by taking partial trace of $\sigma_{U_1U_2W_1E_1E_2}$ over the system U_1, we have

$$\begin{aligned} \sigma_{U_1W_1E_1E_2} &= \sum_{u_1,w_1 \in \mathbb{F}_2} \frac{1}{2} P_{W_1}(w_1) |u_1, w_1\rangle\langle u_1, w_1| \\ &\quad \otimes \left(\sum_{u_2 \in \mathbb{F}_2} P_{U_2|W_1=w_1}(u_2) \sigma^{(u_1,u_2),w_1}_{E_1E_2} \right). \end{aligned}$$

Thus, we have

$$\begin{aligned} H(\sigma_{U_1W_1E_1E_2}) &= 1 + H(P_{W_1}) + \sum_{u_1,w_1 \in \mathbb{F}_2} \frac{1}{2} P_{W_1}(w_1) \\ &\quad H\left(\sum_{u_2 \in \mathbb{F}_2} P_{U_2|W_1=w_1}(u_2) \sigma^{(u_1,u_2),w_1}_{E_1E_2} \right) \\ &= 1 + H(P_{\bar{\mathsf{X}}}) + \sum_{\bar{x} \in \mathbb{F}_2} P_{\bar{\mathsf{X}}}(\bar{x}) H(P_{\vec{\mathsf{X}}\mathsf{J}|\bar{\mathsf{X}}=1}). \end{aligned} \tag{E3}$$

Combining Eqs. (E1) and (E3), we have

$$\begin{aligned} & H_\sigma(U_2|W_1U_1E_1E_2) - P_{W_1}(0) H(P_{W_2|W_1=0}) \\ &= P_{\bar{\mathsf{X}}}(0)(1 - H(P'_{\mathsf{XZ}})). \end{aligned}$$

Lemma 42 Let C be a linear subspace of $\mathbb{F}_2^m$. Let

$$|\varphi^m(\vec{x},\vec{\mathsf{x}})\rangle \frac{1}{\sqrt{P^m_{\mathsf{X}}(\vec{\mathsf{x}})}} \sum_{\vec{z} \in \mathbb{F}_2^m} (-1)^{\vec{x}\cdot\vec{z}} \sqrt{P^m_{\mathsf{XZ}}(\vec{\mathsf{x}},\vec{z})} |\vec{\mathsf{x}},\vec{z}\rangle,$$

and $\sigma^{\vec{x},\vec{x}}_{E^m} := |\varphi^m(\vec{x},\vec{\mathsf{x}})\rangle\langle\varphi^m(\vec{x},\vec{\mathsf{x}})|$. Let J be a set of coset representatives of the cosets $\mathbb{F}_2^m/C$, and

$$P_{\mathsf{J}|\mathsf{X}^m=\vec{\mathsf{x}}}(\vec{\mathsf{j}}) := \frac{\sum_{\vec{\mathsf{c}} \in C^\perp} P^m_{\mathsf{XZ}}(\vec{\mathsf{x}}, \vec{\mathsf{j}} + \vec{\mathsf{c}})}{P^m_{\mathsf{X}}(\vec{\mathsf{x}})}$$

be conditional probability distributions on J. Then, for any $\vec{a} \in \mathbb{F}_2^m$, we have

$$\sum_{\vec{x} \in C} \frac{1}{|C|} \sigma^{\vec{x}+\vec{a},\vec{x}}_{E^m} = \sum_{\vec{\mathsf{j}} \in \mathsf{J}} P_{\mathsf{J}|\mathsf{X}^m=\vec{\mathsf{x}}}(\vec{\mathsf{j}}) |\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})\rangle\langle\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})|, \tag{E4}$$

where

$$\begin{aligned} |\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})\rangle &:= \frac{1}{\sqrt{\sum_{\vec{\mathsf{e}} \in C^\perp} P^m_{\mathsf{XZ}}(\vec{\mathsf{x}}, \vec{\mathsf{j}} + \vec{\mathsf{e}})}} \\ &\quad \sum_{\vec{\mathsf{c}} \in C^\perp} (-1)^{\vec{a}\cdot\vec{\mathsf{c}}} \sqrt{P^m_{\mathsf{XZ}}(\vec{\mathsf{x}}, \vec{\mathsf{j}} + \vec{\mathsf{c}})} |\vec{\mathsf{x}}, \vec{\mathsf{j}} + \vec{\mathsf{c}}\rangle. \end{aligned}$$

Remark 43 If $\vec{\mathsf{j}} \neq \vec{\mathsf{i}}$, obviously we have $\langle\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})|\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{i}})\rangle = 0$. Thus, the right hand side of Eq. (E4) is an eigen value decomposition. Moreover, if $\vec{a} + \vec{b} \in C$, then we have $|\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})\rangle = |\vartheta(\vec{b},\vec{\mathsf{x}},\vec{\mathsf{j}})\rangle$.

Proof. For any $\vec{x} \in C$ and $\vec{a} \in \mathbb{F}_2^m$, we can rewrite

$$\begin{aligned}|\varphi(\vec{x}+\vec{a},\vec{\mathsf{x}})\rangle &= \frac{1}{\sqrt{P_{\mathsf{X}}^m(\vec{\mathsf{x}})}} \sum_{\vec{\mathsf{j}}\in\mathsf{J}} \sum_{\vec{c}\in C^\perp} (-1)^{(\vec{x}+\vec{a})\cdot(\vec{\mathsf{j}}+\vec{c})} \\ &\qquad \sqrt{P_{\mathsf{XZ}}^m(\vec{\mathsf{x}},\vec{\mathsf{j}}+\vec{\mathsf{c}})}|\vec{\mathsf{x}},\vec{\mathsf{j}}+\vec{\mathsf{c}}\rangle \\ &= \sum_{\vec{\mathsf{j}}\in\mathsf{J}} (-1)^{(\vec{x}+\vec{a})\cdot\vec{\mathsf{j}}} \sqrt{P_{\mathsf{J}|\mathsf{X}^m=\vec{\mathsf{x}}}(\vec{\mathsf{j}})}|\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})\rangle.\end{aligned}$$

Then, we have

$$\begin{aligned}&\sum_{\vec{x}\in C} \frac{1}{|C|}\sigma_{E^m}^{\vec{x}+\vec{a},\vec{x}} \\ &= \sum_{\vec{x}\in C} \frac{1}{|C|} \sum_{\vec{\mathsf{i}},\vec{\mathsf{j}}\in\mathsf{J}} (-1)^{(\vec{x}+\vec{a})\cdot(\vec{\mathsf{i}}+\vec{\mathsf{j}})} \sqrt{P_{\mathsf{J}|\mathsf{X}^m=\vec{x}}(\vec{\mathsf{i}})P_{\mathsf{J}|\mathsf{X}^m=\vec{\mathsf{x}}}(\vec{\mathsf{j}})} \\ &\qquad |\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{i}})\rangle\langle\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})| \\ &= \sum_{\vec{\mathsf{i}},\vec{\mathsf{j}}\in\mathsf{J}} (-1)^{\vec{a}\cdot(\vec{\mathsf{i}}+\vec{\mathsf{j}})} \sum_{\vec{x}\in C} \frac{1}{|C|} (-1)^{\vec{x}\cdot(\vec{\mathsf{i}}+\vec{\mathsf{j}})} \sqrt{P_{\mathsf{J}|\mathsf{X}^m=\vec{x}}(\vec{\mathsf{i}})P_{\mathsf{J}|\mathsf{X}^m=\vec{\mathsf{x}}}(\vec{\mathsf{j}})} \\ &\qquad |\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{i}})\rangle\langle\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})| \\ &= \sum_{\vec{\mathsf{j}}\in\mathsf{J}} P_{\mathsf{J}|\mathsf{X}^m=\vec{\mathsf{x}}}(\vec{\mathsf{j}})|\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})\rangle\langle\vartheta(\vec{a},\vec{\mathsf{x}},\vec{\mathsf{j}})|,\end{aligned}$$

where $\cdot$ is the standard inner product on the vector space $\mathbb{F}_2^m$, and we used the following equality,

$$\sum_{\vec{x}\in C} (-1)^{\vec{x}\cdot(\vec{\mathsf{i}}+\vec{\mathsf{j}})} = 0$$

for $\vec{\mathsf{i}} \neq \vec{\mathsf{j}}$. □

APPENDIX F: BELL DIAGONAL STATE IS THE WORST CASE

In this section, we show that the evaluation of the key rate formula for a Bell diagonal state is the worst case. Let σ_{AB} be a two-qubit density operator such that Bell diagonal entries are $\{P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z})\}$, i.e., $\langle\psi(\mathsf{x},\mathsf{z})|\sigma_{AB}|\psi(\mathsf{x},\mathsf{z})\rangle = P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z})$. Let $\{\mathsf{XZ}(\mathsf{x},\mathsf{z})\}_{\mathsf{x},\mathsf{z}\in\mathbb{F}_2}$ be the Pauli operators on the qubit, let $\sigma_{AB}^{\mathsf{s},\mathsf{t}} := \mathsf{XZ}(\mathsf{s},\mathsf{t})^{\otimes 2}\sigma_{AB}\mathsf{XZ}(\mathsf{s},\mathsf{t})^{\otimes 2}$, and let

$$\hat{\sigma}_{AB} := \frac{1}{4}\sum_{\mathsf{s},\mathsf{t}\in\mathbb{F}_2} \sigma_{AB}^{\mathsf{s},\mathsf{t}}$$

be the discrete-twirled operator of σ_{AB}. Note that $\hat{\sigma}_{AB}$ is of the form $\sum_{\mathsf{x},\mathsf{z}\in\mathbb{F}_2} P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z})|\psi(\mathsf{x},\mathsf{z})\rangle\langle\psi(\mathsf{x},\mathsf{z})|$ [41]. Let $\sigma_{U_1U_2W_1E_1E_2}^{\vec{\mathsf{s}},\vec{\mathsf{t}}}$ be a density operator derived from a purification $\sigma_{A^2B^2E^2}^{\vec{\mathsf{s}},\vec{\mathsf{t}}}$ of $\sigma_{A^2B^2}^{\vec{\mathsf{s}},\vec{\mathsf{t}}}$ in the same way as $\sigma_{U_1U_2W_1E_1E_2}$ is derived from a purification $\sigma_{ABE}^{\otimes 2}$ of $\sigma_{AB}^{\otimes 2}$ in Section 2, where $\sigma_{A^2B^2}^{\vec{\mathsf{s}},\vec{\mathsf{t}}} := \sigma_{AB}^{\mathsf{s}_1,\mathsf{t}_1} \otimes \sigma_{AB}^{\mathsf{s}_2,\mathsf{t}_2}$ for $\vec{\mathsf{s}} = (\mathsf{s}_1,\mathsf{s}_2)$ and $\vec{\mathsf{t}} = (\mathsf{t}_1,\mathsf{t}_2)$. Since a phase flip error does not affect the measurement by $\{|0_z\rangle,|1_z\rangle\}$-basis, and since a bit flip error only permutate the indices of measurement results, we have

$$H_\sigma(U_1U_2|W_1E_1E_2) = H_{\sigma^{\vec{\mathsf{s}},\vec{\mathsf{t}}}}(U_1U_2|W_1E_1E_2).$$

Let

$$|\Phi_{ABE\mathsf{STS'T'}}\rangle := \sum_{\mathsf{s},\mathsf{t}\in\mathbb{F}_2} \frac{1}{2}|\Phi_{ABE}^{\mathsf{s},\mathsf{t}}\rangle|\mathsf{s},\mathsf{t},\mathsf{s},\mathsf{t}\rangle$$

be a purification of $\tilde{\sigma}_{AB}$, where $|\Phi_{ABE}^{\mathsf{s},\mathsf{t}}\rangle\langle\Phi_{ABE}^{\mathsf{s},\mathsf{t}}| := \sigma_{ABE}^{\mathsf{s},\mathsf{t}}$. Let $\tilde{\sigma}_{U_1U_2W_1E_1E_2\vec{\mathsf{S}}\vec{\mathsf{T}}\vec{\mathsf{S}}'\vec{\mathsf{T}}'}$ be a density operator derived from $\Phi_{ABE\mathsf{STS'T'}}^{\otimes 2}$ in the same way as $\sigma_{U_1U_2W_1E_1E_2}$ is derived from $\sigma_{ABE}^{\otimes 2}$. Then, by using the strong subadditivity of von Neumann entropy, we have

$$\begin{aligned}&H_{\tilde{\sigma}}(U_1U_2|W_1E_1E_2\vec{\mathsf{S}}\vec{\mathsf{T}}\vec{\mathsf{S}}'\vec{\mathsf{T}}') \\ &\leq H_{\tilde{\sigma}}(U_1U_2|W_1E_1E_2\vec{\mathsf{S}}\vec{\mathsf{T}}) \\ &= \sum_{\vec{s},\vec{t}\in\mathbb{F}_2^2} \frac{1}{16} H_{\sigma^{\vec{s},\vec{t}}}(U_1U_2|W_1E_1E_2) \\ &= H_\sigma(U_1U_2|W_1E_1E_2).\end{aligned}$$

In the similar manner, we have

$$\begin{aligned}&H_{\tilde{\sigma}}(U_2|W_1U_1E_1E_2\vec{\mathsf{S}}\vec{\mathsf{T}}\vec{\mathsf{S}}'\vec{\mathsf{T}}') \\ &\leq H_\sigma(U_2|W_1U_1E_1E_2).\end{aligned}$$

On the other hand, P_{W_1} and $P_{W_2|W_1=0}$ are invariant under the discrete twirling operation. Thus, Bell diagonal state is the worst case for a fixed Bell diagonal entries $\{P_{\mathsf{XZ}}(\mathsf{x},\mathsf{z})\}$.

[1] G. Brassard and L. Salvail, in *Advances of Cryptology – EUROCRYPT '93*, edited by T. Helleseth (Lofthus, Norway, 1994), vol. 765 of *Lecture Notes in Computer Science*, pp. 410–423.

[2] C. H. Bennett, G. Brassard, C. Crepeau, and U. Maurer, IEEE Trans. on Inform. Theory **41**, 1915 (1995).

[3] C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. Computers Systems and Signal Processing* (Bangalore, India, 1984), pp. 175–179.

[4] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998),

arXive:quant-ph/9805019.
[5] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, Proc. 32-nd Annu. ACM Symp. Theory of Computing pp. 715–724 (2000), arXive:quant-ph/9912053.
[6] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, J. Cryptology **19**, 381 (2006), arXive:quant-ph/0511175.
[7] D. Mayers, Journal of ACM **48**, 351 (2001), arXive:quant-ph/9802025.
[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000), arXive:quant-ph/0003004.
[9] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996), arXive:quant-ph/9511027.
[10] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996), arXive:quant-ph/9604024.
[11] H. K. Lo, Quant. Inform. Comput. **1**, 81 (2001), arXive:quant-ph/0102138.
[12] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005), arXive:quant-ph/0410215.
[13] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005), arXive:quant-ph/0502064.
[14] R. Renner, Ph.D thesis, Dipl. Phys. ETH, Switzerland (2005), arXive:quant-ph/0512258.
[15] D. Gottesman and H. K. Lo, IEEE Trans. Inform. Theory **49**, 457 (2003), arXive:quant-ph/0105121.
[16] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002), arXive:quant-ph/0205060.
[17] X. Ma, C. H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H. K. Lo, Phys. Rev. A **74**, 032330 (2006), arXive:quant-ph/0604094.
[18] B. Kraus, C. Branciard, and R. Renner, Phys. Rev. A **75**, 012316 (2007), arXive:quant-ph/0610151.
[19] U. Maurer, IEEE Trans. Inform. Theory **39**, 733 (1993).
[20] J. Bae and A. Acín, Phys. Rev. A **75**, 012334 (2007), arXive:quant-ph/0610048.
[21] A. Acín, J. Bae, E. Bagan, M. Baig, L. Masanes, and R. Munöz-Tapia, Phys. Rev. A **73**, 012327 (2006), arXive:quant-ph/0411092.
[22] K. Vollbrecht and F. Vestraete, Phys. Rev. A **71**, 062325 (2005), arXive:quant-ph/0404111.
[23] H. K. Lo, New Journal of Physics **5**, 36 (2003), arXive:quant-ph/0201030.
[24] S. Watanabe, R. Matsumoto, and T. Uyematsu, in *Proc. of AQIS 2006* (Beijing, China, 2006), pp. 11–12, arXive:quant-ph/0608030.
[25] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, in *Proceedings of the 4th Theory of Cryptography Conference* (Amsterdam, The Netherlands, 2007), vol. 4392 of *Lecture Notes in Computer Science*, pp. 456–478, arXive:quant-ph/0608199.
[26] I. Csiszár, IEEE Trans. Inform. Theory **28**, 585 (1982).
[27] M. Hamada, J. Phys. A: Math. Gen. **37**, 8303 (2004), arXive:quant-ph/0308029.
[28] R. G. Gallager, *Low Density Parity Check Codes* (M.I.T. Press, 1963).
[29] C. Berrou and A. Glavieux, IEEE Trans. Comm. **44**, 1261 (1996).
[30] R. Renner (2007), arXive:quant-ph/0703069.
[31] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley & Sons, 2006), 2nd ed.
[32] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Second Theory of Cryptography Conference TCC*, edited by J. Kilian (Cambridge, MA, USA, 2005), vol. 3378 of *Lecture Notes in Computer Science*, pp. 386–406, arXive:quant-ph/0409078.
[33] R. Renner and R. Konig, in *Second Theory of Cryptography Conference TCC*, edited by J. Kilian (Cambridge, MA, USA, 2005), vol. 3378 of *Lecture Notes in Computer Science*, pp. 407–425, arXive:quant-ph/0403133.
[34] M. Hayashi, *Quantum Information: An Introduction* (Springer, 2006).
[35] D. Slepian and J. K. Wolf, IEEE Trans. Inform. Theory **19**, 471 (1973).
[36] I. Devetak and A. Winter, Phys. Rev. A **68**, 042301 (2003), arXive:quant-ph/0209029.
[37] I. Devetak and A. Winter, Proc. Roy. Soc. London A **461**, 207 (2004), arXive:quant-ph/0306078.
[38] M. Christandl, R. Renner, and A. Ekert (2004), arXive:quant-ph/0402131.
[39] R. Konig, U. Maurer, and R. Renner, IEEE Trans. Inform. Theory **51**, 2391 (2005), arXive:quant-ph/0305154.
[40] J. L. Carter and M. N. Wegman, Journal of Computer and System Sciences **18**, 143 (1979).
[41] M. Hamada, Phys. Rev. A **68**, 012301 (2003).
[42] By applying the random permutation after the transmission phase of QKD protocols, we can assume that Alice and Bob's bit sequences are invariant under the permutation without any compromise of the security.
[43] A $\{ccq\}$-state is a tripartite state such that the first and second systems are classical and the third system is quantum. See [37] for a detail of this notation.